protiviti®
Global Business Consulting

CLOUD SECURITY IN THE UAE

A Security Leader's Perspective

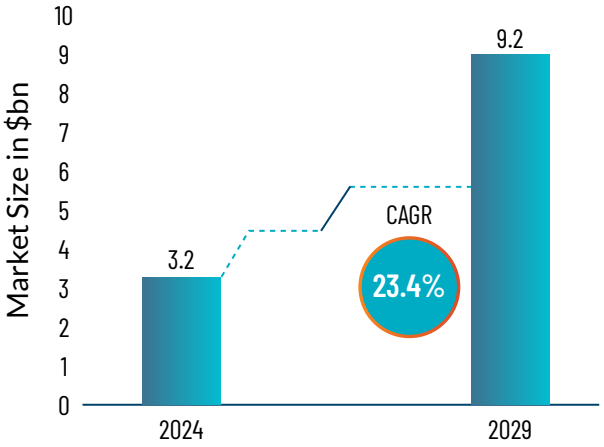
Face the Future with Confidence®

Table of Contents

The State of Cloud in the UAE

The adoption of Cloud computing in the United Arab Emirates has been a journey of rapid growth driven by the UAE Vision 2031, National Artificial Intelligence Strategy 2031 and the strategic ambitions of both public and private sector organizations. Today, cloud computing is the backbone of innovation in the UAE whether its enterprises modernize their infrastructure, enhancing service delivery or exploring the potential of AI and emerging technologies. With current and future investments in Hyperscale data centres, the UAE regulator's forward-thinking policies and focus on data sovereignty and security have created a unique and growing ecosystem leading to technology adoption at an unprecedented rate.

Public Cloud Market Forecast UAE



Source: IDC. United Arab Emirates Public Cloud Market Forecast, 2025–2029.

Cloud adoption in the UAE is being driven by the strong presence of global and regional Colocation and Cloud Service Providers (CSPs), which continue to contribute to the growth of the UAE's digital economy. Major hyperscalers such as Microsoft Azure, Amazon Web Services (AWS), Oracle Cloud Infrastructure (OCI), and others have made significant investments in local data centre regions, delivering resiliency, performance, and scalability to enterprises seeking to accelerate their Go-To-Market strategies. IDC reports that the UAE public cloud market is growing at a CAGR of **23.4%** and is expected to reach $9.2B by 2029.

The Cloud growth is also increasingly complimented are also increasingly complimented by the growing list of Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) offerings leading to organizations being able to build, deploy and scale applications rapidly without the complexity of managing the underlying infrastructure. It is critical to note that alongside global players, regional cloud providers are emerging as critical enablers of sovereign Cloud and industry-specific solutions, creating a competitive landscape and bringing digital solutions closer to their customers and citizens.

Cloud as the Growth Accelerator for Digital Infrastructure

At the very core of cloud computing is the paradigm shift of how organizations can consume, manage and deliver incredible technologies and use cases. At the outset, cost optimization and operational efficiency may seem as obvious benefits, but it is increasingly being recognized as a strategic enabler of agility, scalability and innovation. Today, migration to the Cloud is no longer being viewed from a skeptical viewpoint but as an extension to an organizations data center and computing capabilities. The UAE's public and private sectors have truly embraced this shift and many organizations either have a "cloud-first" or "cloud-only" strategies implemented.

Top Priorities for Organizations in UAE

Source: Balancing Innovation and Compliance in the AI Era Core42 Sovereign Public Cloud Leveraging Microsoft Azure.

With the recent uptick of Artificial Intelligence, specifically Generative AI, Cloud has become one of the most efficient option of choice for fast deployments of AI Use-cases to avoid high investments that often come with the procurement of scarce graphics cards. Hence, organizations are leveraging these capabilities to modernize their legacy systems and support the deployment of cutting-edge technologies, whether it's generative AI, big data analytics or automation, to build resilient digital platforms.

Addressing the Need for Trust and Compliance in Cloud

The UAE's cloud security threat landscape is keeping pace with, and in some ways outrunning its digital ambitions. The IBM Cost of a Data Breach Report 2024 placed the Middle East's average breach cost at $8.75 million, the second highest globally and nearly double the $4.88 million global average, a figure that has climbed year-on year. To tackle this growing complexity, UAE regulators are playing a critical role with their respective frameworks.

First, at the national level, the UAE Cyber Security Council's National Cloud Security Policy (NCSP) provides detailed blueprints and security controls that must be adopted by tenants and providers offering services in the region. It outlines best practices across areas of identity and access management, data protection, incident monitoring and response and many more to serve as a critical reference point for organizations that are transitioning to cloud-based operations.

Shaping the UAE Digital Trust

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Ranked first in the ITU Global Cybersecurity Index 2024, the UAE Cyber Security Council has made cybersecurity a condition of national participation and not a technical discipline left to individual entities. Their "Public-Private-People" partnership distributes responsibility across government, industry and society.

CSC is extending its governance reach into AI Security, IoT and next-generation security operations.

The National Cloud Security Policy (NCSP) provides detailed blueprints and security controls that must be adopted by tenants and providers offering services in the region. It outlines best practices across areas of identity and access management, data protection, incident monitoring and response and many more to serve as a critical reference point for organizations that are transitioning to cloud-based operations.

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

DESC was established with the ambition of making the world's safest digital city and its approach is architectural and not only prescriptive. Its mandate spans government entities, semi-government bodies, critical infrastructure operators, and private sector organizations handling citizen data, with trusted treated as a design principle.

In 2025, DESC launched both, an AI Security Policy and a Zero Trust Assessment Framework, signaling that security must be verified at every layer of the technology stack.

Cloud Security Policy provides detailed technical and governance requirements tailored to the needs of government entities and critical infrastructure operators in the Emirate of Dubai. DESC CSP also mandates Cloud Service Providers to be registered in DESC through a series of mandates and checks that should be evidenced by a CSP prior to initiation of service offerings.

TRA هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY

TDRA's mandate spans the full width of the UAE's digital economy: from spectrum and telecommunications regulation to federal digital government transformation, national cybersecurity response through aeCERT, and data governance under PDPL. Central to its security framework is the UAE Information Assurance Standard (UAE IAS) — the national standard defining the management and technical security controls that government entities and critical infrastructure operators are required to implement and sustain across all ICT systems.

In the cloud, TDRA's approach is equally structured: its IaaS service registration process governs the terms under which Infrastructure as a Service is provisioned within the national digital infrastructure, ensuring cloud services are anchored in data residency, sovereign control, and UAE IAS compliance before being made available to federal entities. For any organisation engaging with the UAE's public sector digital ecosystem, the baseline is non-negotiable: UAE IAS compliant, sovereignty-anchored, and registered before deployment.

As the UAE organizations accelerate their cloud transformation, the regulatory and security landscape is simultaneously growing in depth and complexity. Meeting the requirements of CSC, DESC, ADHICS and emerging privacy legislation is achievable but it demands a structured expert led approach.

This is where Protiviti's Security and Privacy practice has consistently made a measurable difference for organizations across the UAE and the wider region. From designing Zero Trust architectures and conducting Cloud Security Posture assessments, to building regulatory compliance programs and embedding privacy-by-design into cloud native environments. Protiviti brings both the technical depth and the regulatory fluency that complex cloud transformations demand.

Looking Ahead

A Unique Leadership Perspective

This whitepaper was developed to provide a unique and strategic perspective on the evolving cloud security landscape in the UAE, a perspective that seeks the guidance of those who are building, securing and governing the next era of transformation.

To achieve this, we conducted in-depth interviews with 10 distinguished security and technology leaders from public and private sectors across the UAE. These leaders represent diverse industries, including Government, Financial Services, Education, Holding and Healthcare. Through these interviews, we have aimed to capture their deep, firsthand insight into how organizations are approaching cloud adoption at scale. These interviews were conducted during the period of August to December 2025.

In the pages that follow, we invite you to explore the unique perspectives of the UAE's leading security and technology decision makers as they share their successes, challenges and strategic decisions around their respective transformation journeys. Their collective experience offers learnings for any organization that is seeking to harness the full potential of the Cloud, whether it's building Zero Trust Architectures, managing compliance landscapes or leveraging Cloud – native AI capabilities. Though each leader covered in this whitepaper offers their distinct viewpoint of the opportunities and challenges, they share their consensus that Cloud is more than a technology today and has proven to be a strategic foundation to build trusted and resilient platforms.

EISSA NASER AL HAMMADI
Chief Information Security Officer
Department of Health (DOH) – Abu Dhabi

OLIVIER BUSOLINI
Group Chief Information Security Officer
Mashreq Bank

HESSA AL NAHDI
Digital Transformation Leader
Abu Dhabi Heritage Authority

SHAFIULLAH ISMAIL
Sr. VP – Head of Cybersecurity and Risk Unit
Global Asset Management Company

SUMIT DHAR
VP – Information Security
Space42

HARSH DAFTARY
Head of Cloud Security
Large Banking and Financial Services Organization

AMINA ABDULRAHIM
Executive Director of ICT and IT Security
American University of Sharjah (AUS)

NITIN SHINGARI
Director - Cybersecurity
Large UAE-Based Holding Company

KAUSER MUKERI
Chief Information Security Officer
GEMS Education

ABHINAV KUMAR
AVP – Information Security
NMC Healthcare

LEADERSHIP SPEAKS

protiviti®

EISSA NASER AL HAMMADI
Chief Information Security Officer
Department of Health (DOH) – Abu Dhabi

> Embed security from day one, treat identity as the new perimeter, invest in visibility, and just as importantly, build strong partnerships across the business

Q. Where are you currently in your cloud journey?

We are in an advanced hybrid cloud /on premise stage, where security, governance, and resilience are deeply integrated into every cloud and on-premises workload. Our main aim is to lead the way in building a zero trust, identity-focused environment that not only complies with federal standards but also supports sovereign controls. This approach gives us a solid base for launching major digital healthcare projects and keeps us at the leading edge of industry innovation.

While we prefer not to disclose exact percentages, our approach to cloud adoption is anything but arbitrary. Each workload's journey to the cloud is carefully mapped, guided by a dynamic interplay of business priorities, scalability demands, data sensitivity, and requirements for data sovereignty. Instead of one-size-fits-all migration, we embrace a risk-based strategy ensuring every move to the cloud is deliberate, secure, and aligned with our vision for digital excellence.

Considering the sensitive nature and criticality of our industry we adopt a hybrid environment. The model was intentionally designed to balance security, agility, and regulatory compliance while maintaining flexibility to adapt to emerging needs.

The key business drivers were agility, cost optimization, scalability, regulatory compliance and the ability to leverage data and AI capabilities for smart decision making. In the UAE government and healthcare sector specifically, security and data sovereignty were critical drivers, especially with sensitive health information and geo-political considerations. We had to ensure any cloud adoption met with strict national regulations like UAE-IA, Federal Decree Law No.45 of 2021 and Law No.2 of 2019, ADHICS and so on. Security wasn't an afterthought, it was a foundational part of the strategy guiding our selection of trusted cloud partners and the design of layered, zero-trust architectures.

Our approach to cloud adoption is fundamentally shaped by a robust compliance framework that brings together both international best practices and local regulatory mandates. Our strategy incorporates UAE Information Assurance Standard (IAS), Sovereign Controls, and the Minimum Cybersecurity Assurance Framework (MCAF). On a legislative level, we ensure full compliance with Federal Law No. 2 of 2019 and Federal Decree-Law No. 45 of 2021, both of which set clear expectations for handling sensitive healthcare data from within the UAE. Our architecture and operational posture strictly adhere to global benchmarks such as ISO/IEC 27001:2022, NIST SP 800-53 and SP 800-171, as well as Cloud Security Alliance's Cloud Controls Matrix (CSA CCM). For healthcare sectors of Abu Dhabi, we use ADHICS v2 (which was released last year by DoH) as the standard which includes Cloud Security and Data Privacy.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

One of the biggest challenges was maintaining consistent security and compliance across a complex, hybrid environment, while still enabling the business to move at speed. Cloud platforms evolve rapidly, and it was critical for us to ensure that our security controls remained dynamic and adaptive, rather than static and perimeter bound.

Managing third-party risks was another challenge we encountered during our transition to cloud service particularly with SaaS/PaaS solutions and cloud-native integrations. To address this, we conducted comprehensive vendor and third-party risk assessments prior to any integration or usage, which involved in-depth technological risk evaluations to ensure compliance.

Embedding security into every phase of cloud adoption, from architecture design to ongoing operations, and by investing in zero trust models, and real time threat detection, we have successfully turned these challenges into opportunities to further strengthen our cybersecurity posture.

Misconfiguration, insufficient segmentation, and lack of telemetry are generally considered challenges. These issues often arise in fast-evolving hybrid and multi-cloud environments. Our recommended approach includes implementing policy-driven access controls, adopting micro-segmentation to limit lateral movement, and embedding continuous threat modelling into the architecture. We've also prioritized enhancing incident response capabilities tailored for hybrid deployments, ensuring that visibility and agility remain central to our security posture.

One of the key lessons we've learned is that security must be built into the cloud journey from the very beginning and not thought of afterwards. Securing cloud workloads shifts from the traditional perimeter-based thinking to a zero trust, workload centric model, where every identity, device and workload must continuously prove their trustworthiness.

Visibility is non-negotiable, you cannot protect what you cannot see. Investing early in a centralized SIEM and strong red teaming made a significant difference. Finally, the organization must shift along with you. We introduced Data Privacy and DevSecOps champions to ensure security is embedded into the organizational mindset. Having a shared responsibility with business is critical to sustaining security at scale.

Advice to other CISOs / CIOs:

Embed security from day one, treat identity as the new perimeter, invest in visibility, and just as importantly, build strong partnerships across the business. Cloud security is not owned by security teams alone: it's a shared responsibility model.

Q. How do you balance security and privacy in a hybrid environment?

We apply a unified, risk-based approach to data classification and protection, ensuring consistency across both on-premises and cloud environments. Classification follows Abu Dhabi Government Data Classification Standard.

We leverage automation tools such as data discovery, labelling, and rights management solutions to ensure sensitive data is identified, classified, and protected at the point of creation, regardless of location.

Protection mechanisms like encryption at rest, in use and in transit, tokenization, access controls based on least privilege, data masking, differential privacy and continuous monitoring are enforced uniformly across all environments. This is a continuous journey and improved over time.

We align our security and data governance frameworks to UAE-specific regulations such as UAE-IA, Sovereign Controls, and emerging privacy laws. Compliance is integrated into our cloud and infrastructure design from the outset, not treated as a checkbox exercise. We maintain continuous compliance monitoring, perform regular risk assessments, and work closely with our legal and regulatory experts to stay ahead of changes in the regulatory landscape.

One key gap is the difference of application of security policies between legacy and cloud systems. Traditional on-premises controls often do not automatically extend into cloud-native architecture. We addressed this by establishing unified security policies, enhancing identity and access management, and deploying cloud security technologies like CSPM and CNAPP and log monitoring to ensure seamless control across environments.

Identity is the new perimeter. We use a centralized identity platform that federates access across cloud and on-premises assets, enforce strong multi-factor authentication (MFA), least privilege access models (PIM), continuous authentication, and role-based access controls (RBAC). Privileged accounts are further protected with PAM (Privileged Access Management) solutions, ensuring robust governance.

Q. How do you effectively manage CSP and CSP Platforms?

Vendor risk management follows a structured assurance lifecycle:

- Pre-engagement due diligence with detailed risk assessments.
- Cloud contract scrutiny for residency, incident response, and exit clauses.
- Technical assessments mapped to DoH Security requirements.

Before onboarding, we validate the CSP's compliance with UAE regulations, research any previous incidents, assess their security and privacy controls, review their data residency and sovereignty guarantees, conduct architectural reviews, and ensure contractual obligations include incident response, breach notification, and audit rights. Only after satisfactory security and governance indications may we commence the engagement.

We maintain visibility through continuous security monitoring tools, cloud-native security services (such as Cloud Security Posture Management), SIEM and XDR integrations. We also emphasize independent validation of CSP security controls on a periodic basis.

While specific tools remain confidential, our approach includes:

- Threat modelling aligned with MITRE ATT&CK.
- Cloud security validation per NIST CSF and CSA CMM.
- Regular technical assessments and continuous monitoring.

Q. What are your thoughts on looking forward to Cloud?

The biggest emerging threat is the exploitation of identity and machine identities at scale, especially with the rise of automation, APIs, and AI agents. Also, with the use of AI, Data reidentification increases. As cloud environments become more dynamic and decentralized, protecting every identity—human and non-human—will be the critical battleground. Another potential threat would be supply chain compromises through third-party integrations.

AI will enhance predictive threat analysis, anomaly-based detection, and auto-remediation. Automation will play a major role in compliance enforcement, drift detection, and posture scoring. However, governance of AI models (ensuring transparency and fairness) will emerge as a critical security domain in its own right.

We are focusing on expanding zero trust architectures, investing in cloud-native threat intelligence platforms, automating compliance reporting, and upskilling teams with cloud security certifications and cyber drills that simulate cloud-native scenarios. We are also enhancing incident response capabilities, specifically tuned for hybrid and multi-cloud environments.

A major shift in cloud security will be the move from static compliance checklists to real-time assurance. Cloud platforms will need to demonstrate continuous compliance through integrated, measurable controls that reflect both security and data sovereignty posture. Traditional notions of "inside" and "outside" the network will dissolve entirely, and security will follow the identity, workload, and data everywhere. Security will become identity-centric.

HESSA AL NAHDI
Digital Transformation Leader
Abu Dhabi Heritage Authority

> Security in the cloud is not just about leveraging technology, it's about Governance, Awareness and Accountability at every level

Q. Where are you currently in your cloud journey?

We have adopted a **cloud-only strategy**, with our current environment operating entirely on cloud infrastructure. While this provides clear advantages in scalability, flexibility, and cost efficiency, it also introduces new risks that must be carefully managed.

As an organization with **100%** cloud-based workloads, it is our top priority to ensure resiliency and security. To fully realize the benefits of cloud platforms, we are focusing on **modernizing our cloud environment** and expanding our adoption of technologies that are purpose-built for cloud operations. Our goal is to achieve the right balance between traditional and modern architectures, enabling us to selectively adopt SaaS solutions that deliver value while minimizing our operational risk.

Over the next two years, we aim to execute a **modernization roadmap** that enhances our cloud infrastructure, integrates advanced analytics capabilities, and ensure thatall solutions align with our technical and security requirements.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

Operating in a fully cloud-based environment has brought forward significant lessons and challenges. One of the most notable hurdles has been the **limited availability of cloud security skills**, which slows down implementation and optimization efforts. Additionally, **SaaS offerings remain relatively initial** (with more global SaaS providers initiating offerings locally). This often requires extensive customization to meet standard requirements set forth by regulators. Many providers still lack **clear transparency on data security controls**, making it difficult to validate how customer data is being protected.

To address these concerns, we have implemented **strong governance mechanisms** for cloud security. Our approach includes integrating **security requirements into product evaluation questionnaires**, enabling product owners to assess whether each cloud service provider's (CSP's) controls align with our internal standards. **Availability and connectivity** have also emerged as a challenge, especially when multiple critical services are hosted on a single platform.

For fellow security leaders beginning their cloud journey, our key recommendations are:

- **Retain control over your data's security governance** — ensure your controls, not the provider's defaults, define how your data is protected.
- **Adopt a multi-cloud strategy** to avoid dependency on a single provider. While this adds operational complexity, it significantly improves resilience and availability.
- **Establish clear data recovery and exit strategies** with your CSPs to ensure business resiliency is prioritized.

It is very critical to realise that while CSPs provide the infrastructure, **the accountability for security, compliance, and operational integrity remains with the organization itself.**

Q. How do you balance security and privacy in a hybrid environment?

In a hybrid cloud environment, maintaining the right balance between **security and privacy** is essential. Our approach has been tailored to include **Zero Trust architecture** as a baseline to our **multi-cloud strategy** aiming to strengthen resilience, minimize dependency, and reduce potential points of failure.

From a privacy perspective, we started by **identifying relevant local regulatory requirements** while also **benchmarking against the GDPR**. Our privacy policy has been aligned with these controls to ensure comprehensive protection of personal data. Transparency is a key principle — we have made our privacy policy publicly available on our website, helping customers understand the measures we take to safeguard their information and, in turn, fostering a culture of trust.

Equally important is **employee and leadership awareness**. We consistently take the lead to educate staff and key management about emerging risks and the steps required to stay secure in this incredibly digital world. By empowering employees to practice good security hygiene in both their personal and professional lives, we build a stronger, more privacy-conscious organizational culture.

Q. How do you effectively manage CSP and CSP Platforms?

To ensure alignment between our internal security practices and those of our Cloud Service Providers (CSPs), we have developed **customized assessment questionnaires**. These are used to validate that each CSP's security and operational controls meet our organizational standards. While we occasionally face **challenges in obtaining complete transparency**, we work collaboratively to obtain the necessary assurances, including thorough third-party attestations and documented evidence.

We also employ **technical validation** tools to independently confirm that the configurations and controls applied within CSP environments remain secure and compliant. However, this is only possible in select deployment models.

Another key component of CSP management is the **alignment of contractual terms and conditions**. Given the fast-evolving nature of cloud environments, agreements must be flexible enough to support collaboration while still conforming to **local regulatory requirements**. For instance, just as mobile manufacturers customize their offerings to meet local regulations across different regions (such as the U.S., China, and the UAE), CSP services and terms must also be tailored to the **UAE's legal and regulatory framework** through their compliance with local regulations such as the Cyber Security Council's National Cloud Security Policy.

By combining structured due diligence, contractual governance, and technical assurance, we maintain effective oversight of our CSPs and ensure their operations remain consistent with our compliance and security expectations.

Q. What are your thoughts on looking forward to Cloud?

As cloud adoption continues to accelerate, organizations will experience not only greater opportunities but also an expanding range of risks. Cloud has now become a **foundational element of enterprise IT**. As businesses grow in scale, each will need to adopt **tailored approaches** to safeguard their environments — such as structured **cloud security questionnaires** and continuous assurance mechanisms.

The next phase of cloud evolution will see broader adoption of **AI-driven services, SaaS platforms, and advanced automation**, along with deeper **collaboration between providers and customers**. Leveraging **AI for cloud infrastructure management** will become increasingly common, enabling more intelligent monitoring, optimization, and response capabilities.

In summary, as cloud ecosystems evolve and interconnect further, organizations must strengthen their **governance and security frameworks combined with strong architecture foundations** to stay resilient, compliant, and ready to embrace the innovations that the next generation of cloud services will bring.

SUMIT DHAR

VP – Information Security

Space42

> In the cloud, security maturity is no longer about preventing identified issues. It's about anticipating failure, protecting what matters most, and building resilience for continued business.

Q. Where are you currently in your cloud journey?

Space42 operates a hybrid cloud model integrating on-premise infrastructure with public cloud platforms. We view cloud as a strategic enabler of resilience, scalability, and business agility, supported by disciplined governance and architecture.

Our adoption focuses on three outcomes: operational efficiency, elastic scalability through hyperscale platforms such as AWS, Azure, and Google Cloud, and financial flexibility through a consumption-aligned operating model.

Our transition followed a structured assessment across application maturity, workload readiness, and regulatory and contractual obligations. This enabled early identification of constraints and informed the definition of a target-state architecture and cloud operating model with clear governance and performance metrics.

The result is a hybrid architecture that balances flexibility with centralized oversight, embedded into our delivery lifecycle to support long-term growth, security, and operational excellence.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

Hybrid and multi-cloud strategies consistently surface challenges across talent, configuration management, visibility, and identity governance.

- **Talent** — Recruiting the right talent is crucial. Secure multi-cloud environments require deep cross-platform expertise and cloud-native security engineering. Structured upskilling, embedded security within engineering teams, and partnerships with specialized providers strengthen execution capacity.
- **Configuration risk** — Misconfigurations remain a leading cause of cloud incidents. Infrastructure-as-Code, automated policy validation, and CI/CD-integrated guardrails reduce drift and enforce consistency at scale.
- **Visibility** — Containerized workloads, serverless architectures, and short-lived compute instances reduce the effectiveness of traditional perimeter-based monitoring tools. Cloud Security Posture Management (CSPM) tools, alongside structured assessments using solutions such as Scout Suite and Prowler, enhance benchmark alignment and proactive detection.
- **Identity** — Identity functions as the primary cloud control plane. Zero Trust principles, centralized IAM governance, and strong federation models reduce exposure across hybrid environments.

The core lesson: cloud security is architectural. Governance, automation, and metrics must integrate directly into engineering and align with business risk priorities.

Q. How do you balance security and privacy in a hybrid environment?

Security and privacy rely on consistent foundational controls across environments. We anchor our approach in least privilege, defense-in-depth, vulnerability management, segregation of duties, continuous monitoring, and strong IAM governance.

Hybrid complexity requires additional emphasis on automated configuration management, cloud-native security tooling, and continuous posture monitoring within the shared responsibility model.

While implementation mechanisms vary between on-premise and cloud, our security standards, privacy thresholds, and risk appetite remain consistent, supported by real-time oversight and measurable control effectiveness.

Q. How do you effectively manage CSP and CSP Platforms?

We manage CSPs through a structured, risk-based framework integrating security controls, governance, monitoring, and vendor oversight.

We combine native capabilities such as Microsoft Defender, XDR, and Entra ID, with vendor-agnostic tools including Scout Suite and Prowler to maintain consistent posture management.

Centralized logging and telemetry enable unified monitoring, expanded detection of cloud-native attack vectors, and CSP-specific response playbooks. Policy-as-code, defined ownership models, and automated guardrails enforce governance at scale.

Effective CSP management requires architecture discipline, automation, and continuous oversight executed within a unified security operating model.

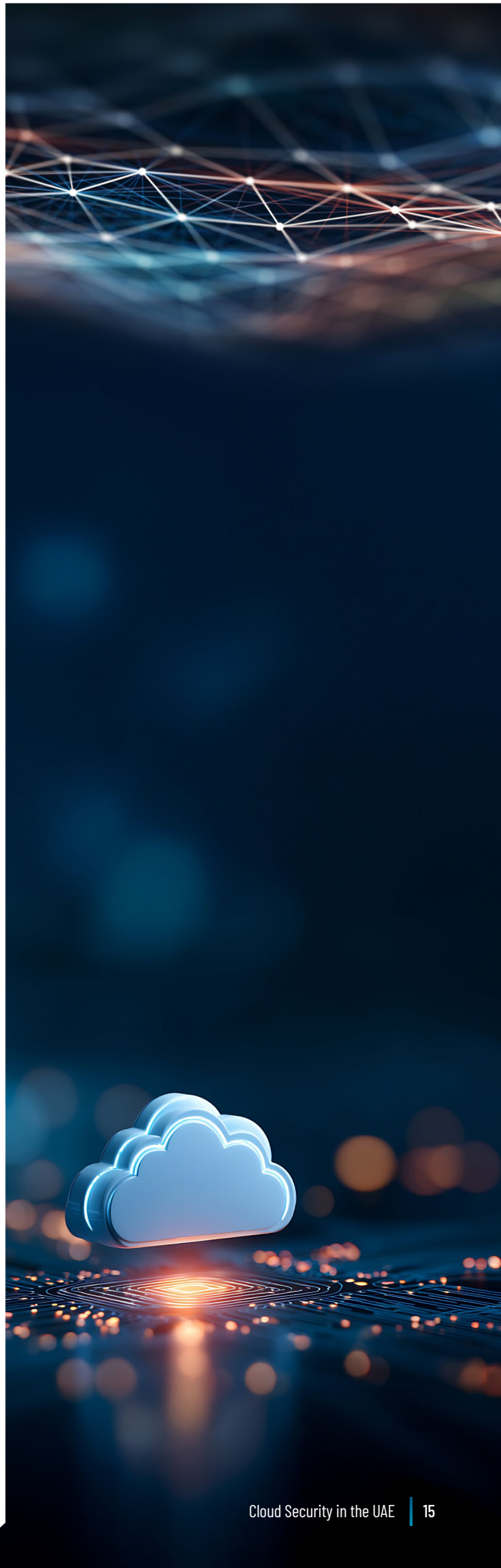
Q. What are your thoughts on looking forward to Cloud?

To be able to discuss the future of cloud security, it is important to understand its evolution. Cloud security has matured from a lift-and-shift replication of on-premise controls to cloud-native posture management, addressing misconfiguration and policy drift through CSPM, CWPP, and CASB.

Today's phase reflects three structural shifts:

- Risk-based prioritization, incorporating exploit likelihood metrics such as EPSS.
- Security embedded by design, through Infrastructure-as-Code, policy-as-code, and CI/CD-integrated guardrails.
- Identity as the control plane, with continuous verification, adaptive MFA, and strong workload identity validation.

Looking ahead, resilience engineering will define the next stage. Architectures will assume failure and automate recovery. Security, reliability, and business continuity will operate as one system to sustain innovation and trust.



AMINA ABDULRAHIM

Executive Director of ICT and IT Security

American University of Sharjah (AUS)

> Effective communication with non-technical management combined with proactive exploration of new technologies can be a powerful enabler for businesses.

Q. Where are you currently in your cloud journey?

About a decade ago, the idea of moving to the Cloud felt incredibly risky, especially for AUS. Cloud as a concept was still new, with limited cloud service providers offering services; in general, the perception was that physical infrastructure was comparatively safer. Many believed that keeping things on-site meant more control and better security.

As one of the most prominent universities in the UAE, ***GROWTH*** has been a key driver for us, whether from a student's perspective or from a business perspective. For our students, it is extremely critical for them to be exposed to cutting-edge technologies, and we could see the benefits of adopting Cloud for this scalability purpose, as a wide array of technology is readily accessible. This demand in the business and education sectors really led AUS on the journey to adopt multi-cloud systems early on.

As we moved forward, we started to see benefits we had not fully anticipated. We saved time, reduced reliance on short-life or single-use hardware like local storage devices and monitoring equipment and gained flexibility in how our organization worked.

As we moved forward in our cloud transition journey, we witnessed the ease of system upgrades, patch management and scaling when compared to a legacy infrastructure. These had been a painful administrative task to manage due to the distributed nature of our infrastructure. With a current cloud consumption of about **40%** on Cloud, we aspire to move **70%** on Cloud within the next three years.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

As we moved ahead into our cloud journey, AUS came across challenges that kept shifting almost as fast as the technology itself.

One of the first hurdles was **getting the value realization right**. It is often a valid assumption that moving to the Cloud should lower costs, but in reality, managing spend and expectations is a constant balancing act and can spiral out of control if not consistently monitored.

We had to strategize the multi-cloud approach to better manage the **evolving student and business expectations**, which led us to pay careful considerations around security and ensure that data remains within acceptable jurisdictions.

As we moved forward in our adoption journey, we also realized that **contractual obligations** were not always in our favor and reading large contractual documents can be taxing when getting started is a priority. In one case, shutting down a cloud application came with an early-exit fee despite no contractual breaches, as vendor lock-in risks were quite substantial in the early days of Cloud.

One of the ongoing challenges that requires consistent attention is addressing **internal knowledge gaps** around hybrid security controls. To tackle this, we inculcate training and knowledge transfer as an integral part of the migration activity rather than relying solely on certifications. We also bring in external experts for ethical hacking exercises and third-party assessments, which help uncover blind spots, strengthen our posture, and transfer valuable skills to our team, boosting knowledge retention and reducing turnover.

From all this, a few lessons stood out for us:

- Make data security and classification part of the plan initially and intentionally.
- Keep a close eye on consumption to avoid cost surprises.
- Go in with a clear strategy, but stay adaptable to the changing technology.
- Look at the long-term value, not just the initial migration.

Q. How do you balance security and privacy in a hybrid environment?

We realize that it is almost impossible to baseline security and privacy controls perfectly across both multi-cloud and on-premises systems. Instead of aiming for identical setups, we focus on creating a **consistent baseline of protection across all applicable layers**. Firewalls and orchestration layers help us streamline operations between environments, so security standards remain strong regardless of where workloads are located.

Meeting UAE regulations and laws, CSC guidelines, and sector-specific regulations can be complex, but it is non-negotiable. For instance, we follow the **UAE National Cloud Security Policy** and apply a **risk-based governance model** that clearly defines responsibilities for both cloud providers and consumers. We also align with the **UAE Information Assurance Regulations**, implementing standardized, appropriate security controls along with continuous risk-driven monitoring and evaluation.

Identity and access management is an absolute must in our hybrid environment, which includes multiple CSPs and on-site legacy systems. We are also developing a **unified identity management layer** to handle authentication and permissions consistently across all platforms.

Everything AUS does is guided by a **"trust but verify" approach**. We trust our systems and people, but we also embed verification processes to ensure accountability, integrity, and compliance across the entire hybrid architecture.

Q. How do you effectively manage CSP and CSP Platforms?

AUS takes a structured and proactive approach to managing our Cloud Service Providers (CSPs) and platforms, making sure security is embedded into every stage — from procurement to ongoing operations.

Each CSP is managed using its own native security tools. We maintain separate, provider-specific dashboards to monitor risks and controls for each platform. This gives us extensive visibility into individual environments. However, we have not yet consolidated everything into a single unified view, but have that planned for the near future to baseline our security monitoring.

To manage vendor risk, security requirements are built directly into the **procurement and tendering process**. Any vendor that cannot meet those requirements is disqualified at onboarding. We also use a formalized security checklist, based on the **HECVAT**, to assess key areas like access controls, patch management, and vulnerability handling.

We strongly emphasize compliance with standards such as **SOC 2 Type 2**, requiring vendors to provide evidences of compliance to build a nature of trust with the CSP.

By taking a controlled and incremental approach, AUS ensures that each platform is managed according to its unique needs, while keeping a broader consolidation strategy on the horizon. This balance allows us to unify governance over time, maintain financial stability, and uphold security without compromising clarity or compliance.

Lastly, with a shift in the skills landscape, multi-cloud proficiency has become a baseline requirement for our teams. We are considering strategically moving certain infrastructure layers from internal operations to managed services, allowing us to concentrate on enhancing system security and architecture while increasing efficiency and business resilience.

Q. What are your thoughts on looking forward to Cloud?

As we see it, one of the biggest challenges for security leaders will be managing security as the technology stack grows in complexity. The Cloud continues to evolve at a rapid pace, and each new capability brings fresh risks. For instance, AI use cases and POCs are a driving demand, so the adoption of AI delivered through the Cloud is part of a natural augmentation of infrastructure. However, AI models deployed on the Cloud will now add another layer of complexity to securing these environments.

To prepare for this, we must consistently apply the time-proven principles of a security-by-design approach. Since security is no longer an afterthought, critical controls like Data classification, secured identity management, security monitoring and risk assessments should be carried out during the design and procurement phases, ensuring alignment with both the UAE's regulatory requirements and the internal governance models of AUS.

While we recognize that moving to the Cloud doesn't automatically translate into cost savings, the scalability and agility it offers make it an essential part of our long-term strategy to bring cutting-edge innovation to our students and future generations.

KAUSER MUKERI

Chief Information Security Officer

GEMS Education

Q. Where are you currently in your cloud journey?

The cloud journey in the region began a few years ago with a hybrid strategy. I have worked at several banks and now at GEMS Education, and each organisation approaches cloud adoption differently. Ten years ago, everyone was talking about cloud as the future, but many were not ready, particularly in regions like ours, where data sovereignty and hosting were significant concerns. However, that changed once local cloud data centres were established. With support from security tools like encryption and bring-your-own-key, technical teams as well as leadership started to gain confidence. The pivotal factors were cost and scalability. At GEMS, we operate over 45 schools with a significant on-premises infrastructure, so our current model is roughly **50%** on the cloud.

We are steadily migrating services to the cloud, especially where scale and shared resources are logical. Cloud-first strategies are now on the table for most organisations, and we are no exception.

The pandemic accelerated cloud adoption. In the banking sector, the security architecture upgrades were completed when remote working became essential. In the education sector, the shift was even more urgent, as students needed to continue essential education online. We had to quickly deploy virtual classrooms, secure remote access, and ensure continuity for students and staff. Cloud was the only solution that made this possible at speed and scale, and for many organisations, that urgency removed prior hesitation and fast-tracked the cloud journey.

> With technology evolving fast, what we implement today might be outdated in a month, so we must stay adaptable and consistently re-assess the risk landscape.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

One of the biggest lessons I have learned, both in banking and at GEMS, is that you have to get the fundamentals right. There is a tendency to chase the latest trends, like AI and automation, but without strong foundations, such as access controls, audit trails, and structured processes, you are leaving critical gaps unaddressed. Security must start with the basics and evolve from there. At the same time, security leaders today must be enablers in a balanced approach. Especially in education, where access is essential for learning, we must support business needs while managing risks. A risk-based approach is key. Not every risk can be eliminated, but with proper mitigation or compensating controls, they can be managed responsibly.

A growing challenge now is around AI. While most organisations are speedrunning use cases, which in our case includes both staff and students, we focus on figuring out how to govern AI safely to protect the new generation from unnecessary exposure. People may unknowingly share sensitive information with AI tools that store or process data externally, which could be potentially damaging to their privacy. Our responsibility is to enable innovation but in a filtered, moderated, and well-informed way. Technology is evolving fast, so what we implement today might be outdated in a month. My message to fellow security leaders would emphasise the need to stay adaptable and consistently re-assess the risk landscape.

Another challenge is the use of the hybrid cloud approach. Hybrid environments add another layer of complexity. While they offer resilience, especially during cloud outages, like the CrowdStrike incident in 2024, they also require different implementation strategies. Even if the control objectives are the same, cloud and on-prem systems need to be configured and maintained differently. It takes discipline, skilled resources, and a thoughtful operational model to do both well.

Q. How do you balance security and privacy in a hybrid environment?

Privacy has become a bigger priority across the region. A few years ago, there was not much awareness around privacy, but with regulations like the UAE and KSA Personal Data Protection Law (PDPL) and other GCC privacy laws now coming into force, organisations are starting to take it more seriously. We are witnessing a similar evolution to what happened with the General Data Protection Regulation (GDPR) in Europe. At GEMS, we manage a lot of personal data, including student records, so we focus on consent, data-sharing policies, vendor agreements, and awareness-building among internal data owners, like administrators and teachers.

Privacy and security are intricately connected. You can have security without privacy, but you cannot have privacy without security. That means, as custodians of data, we must ensure the data we collect is used responsibly and shared only when necessary. We are also part of a broader supply chain, which is why we need to be cautious about who we share data with and how they handle it. While the prevalent thought is that privacy solutions will fix the issues, it has to be a combination of people, process, and technology.

Q. How do you effectively manage CSP and CSP Platforms?

One of the biggest gaps I often see is the underutilisation of features that CSPs already offer. Each platform, such as Amazon Web Services (AWS), Oracle, Google Cloud Platform (GCP), and Azure, uses its own terminology, which can confuse teams who are not deeply familiar with the ecosystem. This often creates a situation where valuable security features get overlooked. This is a common visibility gap, which can be addressed through a solid relationship with the CSP.

Our approach is to request a full list of available modules, configurations, and best practices directly from the CSP periodically. We then cross-check those against our internal standards and use additional tools where needed. The key is having visibility of every asset and configuration on the cloud. If you do not know what is running in your environment, you cannot secure it. That is why we also implement review cycles, either semi-annually or annually, to keep pace with platform changes. This helps ensure we are using what we already pay for, not overspending on external tools that duplicate existing functionality.

Q. What are your thoughts on looking forward to Cloud?

Cloud will continue to shape the future of IT and security. Its ability to scale, deliver performance, and support innovation is unmatched. The only challenge remains around cost management. Many organisations forget to account for how quickly costs can escalate once you start enabling features like detailed logging, added storage, or high-availability options on the cloud. Proper planning and cost optimisation strategies are essential. However, I also expect CSPs to evolve their pricing models to meet this need as they achieve economy of scale in their offerings.

On the security side, we have come a long way. Most of the early concerns around hosting and access have been addressed. Now, the next wave of risk comes from how AI is integrated with cloud infrastructure. For instance, AI meeting assistants can now capture full transcripts, images, and even screen snaps. These tools are powerful, but they introduce major data exposure risks, especially in the education sector. As we move forward, the challenge will be managing the intersection of cloud and AI, such as adopting new tools, while maintaining strong governance, clear boundaries, and ongoing risk assessments.

OLIVIER BUSOLINI

Group Chief Information Security Officer, Mashreq Bank

Mashreq

> CISOs are always under pressure to go fast, my only advice is when you are going fast, make sure you are headed in the right direction.

Q. Where are you currently in your cloud journey?

The journey to cloud requires security leaders to understand the "WHY of the journey" as that's the fundamental for setting the right strategic direction.

At Mashreq, our journey to cloud has been extremely strategic in nature as our environment has evolved organically. It's been a conscious decision to always think about cloud with the pros and cons while keeping the business context in the centerfold of our decision making with "Where we want to go and where we want to grow". Cloud has proven to be a powerful enabler for us from multiple perspectives such as maintainability, cost, sovereignty and the powerful scalability benefits that are at your disposal. These are incredible tools that have helped us increase our time to market.

With around **50%** on cloud vs on-premise deployment, we continue to leverage cloud for our customized use cases and consistently add more value to our business and customers.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

As an early adopter of the cloud, significantly less talent was available in the market which challenged us to perform substantial internal problem solving. Secondly, when an organization adopts cloud, it's extremely critical for the security leaders to be aware that the attack surface will expand cumulatively and hence architecture and security principles must be adopted at the design level itself.

While there are many advantages to cloud, cost may be a debatable one. A fundamental challenge of overall governance exists in cloud environments, extending beyond security which can often contribute to increase in costs of operation.

Lastly, Shared Security Responsibility Model (SSRM) in cloud is one of the most misunderstood challenges of cloud as consumers often do not fully grasp the level of accountability that is accompanied with the cloud adoption.

To my fellow security leaders, I recommend to 1) Challenge the "Cloud Only" mindset and start with "WHY". 2) Identify and work with your internal and external stakeholders i.e. your business, your customers, your regulators and so on. 3) Build your strategic thinking around – Maintainability, Cost, Flexibility, Security and Resiliency. Lastly, its critical to remember that the ultimate accountability for security and operations remains with the company.

Q. How do you balance security and privacy in a hybrid environment?

The balance while critical to achieve and never truly complete requires transformation across competence, tooling and process. While CSPM solutions offer extreme visibility, each module requires a dedicated team for deployment, configuration and alert management. While cloud controls are conceptually similar to on-premise, they are very different when it comes to implementation.

Operating with a **50%** on-cloud and **50%** on-premise infrastructure presents an extreme challenge for critical security controls on data security, identity management and security management due to the need to manage two different solutions providing disparate inputs often leading to significant efficiency challenges. This requires noteworthy efforts to migrate existing automation from older, more historical systems to newer cloud-based platforms. Catering to privacy regulations on the other hand is relatively easier to manage with a single solution instead.

There is a clear opportunity here for security innovators (specifically for DLP and SIEM) to develop comprehensive solutions that span both on-premise and cloud environments.

Q. How do you effectively manage CSP and CSP Platforms?

Large global CSPs like AWS, Google, Azure and others have developed a lot of automation and many tools to manage the wide scale of their operations. Immense amount of functionality and tools are also provided to the tenants in enabling them to better manage their security, cost and other strategic needs.

The key aspect of managing the CSP and to maximize the available CSP platforms starts with building a strategic partnership with the CSPs. We ensure to meet our strategic CSP partners at least monthly to ensure we work collaboratively towards ensuring we utilize all available paid and subscribed capabilities. This partnership optics has provided us with crucial data points for strategic decisions, such as whether to continue growing in the cloud or opt for on-premise solutions for specific projects. This combined with mandatory upskilling through trainings conducted via the CSPs truly help us in achieving scale of operations and security.

Q. What are your thoughts on looking forward to Cloud?

Globally, there is a trend reversal on cloud where organizations are returning to hybrid models due to rising concerns over cost, security, complexity and sovereignty.

Leonardo Da Vinci said, “Simplicity is the ultimate sophistication”. As the cloud environments grow in complexity with more features, there is a critical need for a layer of abstraction to simplify operations, potentially through “everything as a code” or adopting Artificial Intelligence models. Achieving this simplicity and increasing efficiency is essential for survival. This simplicity is the key to navigating the evolving landscape of cloud.

In summary, Data Sovereignty, Complexity (for enabling business) and achieving simplicity will be the key drivers that will define the future roadmap of cloud in the UAE.

SHAFIULLAH ISMAIL

Sr. VP – Head of Cybersecurity and Risk Unit

Global Asset Management Company

> A successful cloud transformation begins with Governance, requires consistent financial discipline and sustains through continuous innovation.

Q. Where are you currently in your cloud journey?

We started our cloud journey from scratch with a greenfield model, enabling a scalable, secure, and cloud-native infrastructure from day one. We've matured into a highly integrated, agile, and secure environment with strong CI/CD and Zero Trust foundations. Currently, we're expanding into multi-cloud, AI/ML integration, and proactive risk management to support ongoing innovation and scale.

Our primary focus has been to leverage the Cloud to enable our business teams that are massively spread geographically. This focus has now expanded to include our existing multi-cloud adoption paired with AI and machine learning integration on multiple facets of use cases.

This cloud journey and adoption were influenced by key business objectives such as:

- **Business Agility:** The integration of a cloud native infrastructure with mature CI/CD capabilities allows for greater business agility.
- **Quick Active Deployment:** Achieved through establishing a scalable and secure digital foundation from day one through a green field approach.
- **Ease of usage of Zero-trust principles:** These strengthen the security posture as the environment is scaled.
- **Risk Management and Regulatory Compliance:** Allows for easier, confident movement across diverse and evolving jurisdictions.
- **Operational Efficiency:** Enhancing efficiency and financial stewardship has helped achieve a faster availability of technology to our worldwide presence.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

Security and compliance stood out as persistent concerns, especially when navigating diverse regulatory landscapes across multi-cloud environments.

Data governance has been equally complex, as defining ownership, classification, and lifecycle policies was particularly tricky in hybrid setups. This becomes quite challenging to handle in a multi-cloud environment with a heavy emphasis on SaaS products; however, the recent emergence of SSPM (SaaS Security Posture Management) solutions may help resolve the visibility aspect of data to a certain extent.

Integrating legacy systems posed architectural hurdles that required significant modernization to avoid disruptions. Our biggest learning was that embedding security by design—through architecture, automation, and monitoring—was key to long-term resilience. Time-proven and globally recognised frameworks like Zero Trust Network Architecture (ZTNA) and Secure Access Service Edge (SASE) should be an absolute consideration when designing a scalable and secure security architecture.

For CISOs and CIOs, my advice would be to begin their cloud transformation journey with the establishment of strong governance over the cloud environment, ensuring that policies, controls and accountability structures are defined and enforced. This foundation supports the compliance and security objectives while also providing the clarity needed for strategic decision-making. Investing in FinOps capability to manage the risk of cost escalation. Apart from financial discipline, prioritizing organizational upskilling is essential which can empower teams with the knowledge and capabilities to operate, security and consistently innovate in the cloud environment. Combined, these measures can create a balanced approach that addresses risk, cost and capability, laying the groundwork for a successful and sustainable cloud transformation.

Q. How do you balance security and privacy in a hybrid environment?

For a global and financial organization like Global Asset Management Company, paying critical attention to the security/privacy regulations and compliance requirements across the world is an essential starting point due to the regulatory nature of our business. Noncompliance to which can lead to financial risks for the organization.

Further, balancing security and privacy in a hybrid environment where workloads span both on-premise and public Cloud requires a deliberate and compliance-driven approach. In our case, while our workloads operate primarily in the public Cloud, data jurisdiction and residency were critical considerations from the outset due to our global presence.

Lastly, as part of our cloud architecture design, we ensured that data residency requirements were mapped to corresponding regulatory obligations, allowing us to maintain compliance across different regions.

We have also implemented robust data classification and monitoring controls, which have helped us ensure that all information assets are accurately identified, classified and managed based on their sensitivity and criticality. The control and technology enhancement has contributed to an enhancement of our ability to track and understand the data flows across our systems, applications and storage environments, which contributed towards greater transparency into the data lifecycle from creation to archival.

Q. How do you effectively manage CSP and CSP Platforms?

I think that, as a starting point, establishing a stronger relationship with the CSP helps build transparency and a sense of mutual trust.

Managing CSPs and cloud platforms effectively requires strong governance, security by design, and consistent policy enforcement. Due to the scalable nature of the Cloud, things can get out of hand if not monitored and managed appropriately.

Leveraging the existing Cloud Security Posture Management solution provided by the CSP is critical, but it can be tiresome and lead to fatigue from the security engineers since each CSP offers their own. In such cases, organizations can look at customized aggregation of logs to a single SOC platform to increase visibility and reduce fatigue.

Zero Trust is essential, so when onboarding any cloud provider, we start with the integration approach based on our own Zero Trust Framework, which sets the guidelines to be followed. This has tremendously helped in baselining our security-by-design approach in a multi-cloud environment.

Regulatory alignment is another cornerstone for us, especially for organizations operating in highly regulated sectors. Maintaining high security standards not only ensures compliance but also strengthens trust with stakeholders.

Lastly, from a performance and cost perspective, CSPs deliver significant value when they take a proactive approach to assess workload requirements and identify opportunities to decommission underutilized resources. These orchestration controls help free up critical compute capacity and help realize an improved return of investment. However, it is equally important to conduct periodic cost assessment to maintain visibility into over consumption, leading to spending that remains aligned with business objectives. This ongoing vigilance allows organization to implement the right governance controls promptly and hence mitigate the risk of escalating cost.

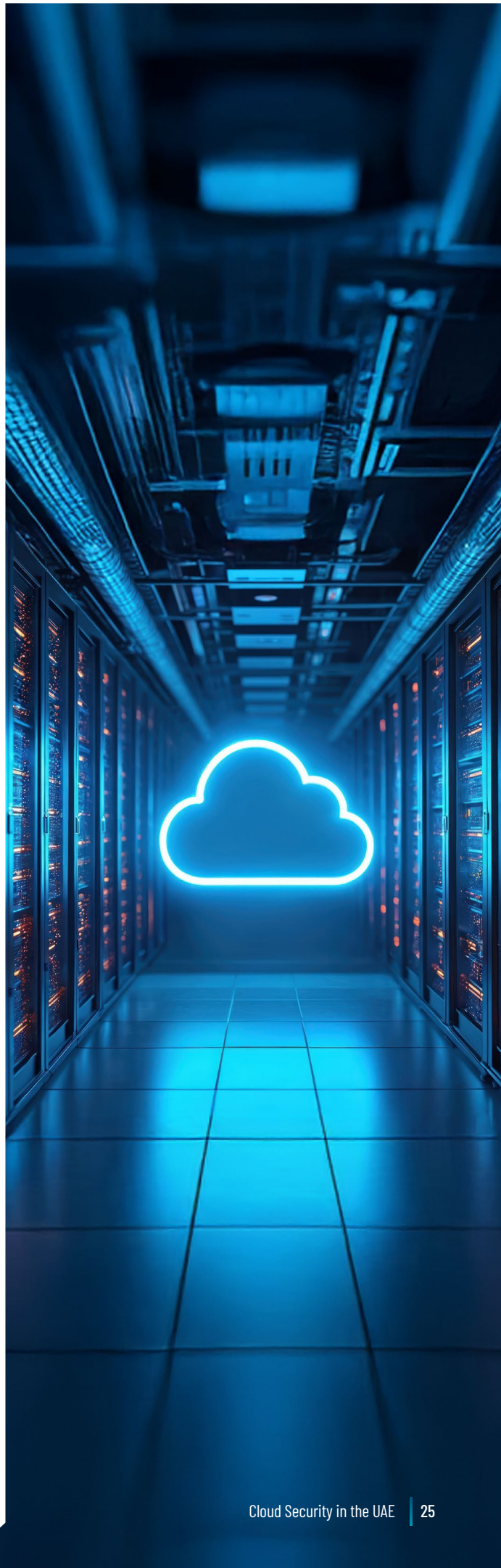
Q. What are your thoughts on looking forward to Cloud?

Looking ahead, the future of cloud security will be shaped by a growing need for automation, intelligence, and adaptability, enabling organizations to remain ahead in an increasingly complex and dynamic threat landscape. As cloud adoption grows, security will shift from reactive to predictive and autonomous models, powered by AI and machine learning for real-time threat detection and response.

Identity-centric security and Zero Trust Architecture will become foundational as traditional network perimeters dissolve. The rise of multi-cloud and hybrid environments will demand unified, cross-platform security strategies and integrated frameworks for compliance, observability, and posture management.

Evolving privacy regulations will require organizations to adopt a “secure by design” approach. Meanwhile, DevSecOps and Infrastructure as Code (IaC) will be essential to embedding security early in the development lifecycle.

In short, cloud security will become smarter, more proactive, and deeply integrated into both technology and business strategy.



HARSH DAFTARY

Head of Cloud Security

Large Banking and Financial Services Organization

> The challenge isn't whether the cloud works but how we can tactfully comply with regulatory expectations in every market

Q. Where are you currently in your cloud journey?

As a large financial entity with a massive geographic presence, leveraging the Cloud has been a cornerstone strategy for us for a much faster go-to-market. Today, we're about **90%** cloud-native, with **60 to 65%** of workloads on private Cloud and the rest on public cloud environments. The key business driver for the Cloud has been our presence across seven geographies and meeting the compliance requirements of over 14 regulators. However, in certain geographies, we get locked into specific available CSPs, which can be quite challenging.

Our SaaS journey is ongoing but challenging due to the absence of a globally defined shared responsibility model, and each CSP defines their own models. For instance, Fusion on OCI, Office 365, Salesforce and Slack all require different implementation approaches despite being labelled as SaaS. We, as a large financial institution, strategize to engineer our own solutions to create a competitive differentiator rather than relying on standard SaaS offerings that provide the same features to all customers.

When we adopt any CSP, we don't utilize their in-built security solutions but define the technology stack ourselves to maintain a uniformity across on – premises and Cloud. Hence, we prefer cloud service providers which give us the freedom of bare metal services and underlying hyperscale infrastructure so we can avoid vendor lock-in from native services, as they do not blend well with our hybrid or multi-cloud strategies.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

One major learning is that cloud providers aren't perfect. We've found and reported serious security bugs in major cloud service providers, where our teams have also been rewarded with finding critical zero-day vulnerabilities. With so many CSPs in the region, they can often release products that aren't fully tested, leading to severe security issues, and most customers just trust the upgrades without doing their own validation. We do not take provider assurance at face value and perform our own thorough assessments before any such upgrades.

Moreover, we don't assume a service will portray uniform behavior across regions. For instance, we found a CSP's network security rules worked differently in India vs the UAE, with the same configurations but different results, so it's extremely critical to anticipate regional inconsistencies.

Equally Important is to have deep discussions with the cloud provider's architects. Your internal design might not work as expected in their environment, so getting your architecture reviewed by their support and services team can help ratify designs and ensure they are technically feasible before deployment.

Lastly, it's critical to rethink security processes as traditional processes, such as vulnerability management, must be completely re-evaluated to be effective in a cloud environment.

Q. How do you balance security and privacy in a hybrid environment?

Balancing security and privacy in a hybrid environment is more of a technical challenge, as CSPs often bring their own standards and controls, making cross-integration quite challenging. For instance, Microsoft has seven or eight ways to encrypt a Virtual Machine,

while AWS has two, and each Cloud only works with its own key management system. So, in this case, even if you generate your own keys, you still have to hand them over to the provider's vault, which makes the cross-cloud consistency extremely challenging. To resolve this, we follow a "bring your own key" model, which gives us some control. On the contrary, the "Hold your own key" model may sound good in theory, but it lacks practicality as it adds latency and complexity, especially when data moves across regions.

Our wide geographical presence has also made privacy trickier, where regulators in countries like Egypt, Saudi Arabia and India are now demanding data sovereignty. That's a complete shift from the centralization trend we saw a decade ago and we're back to distributed models, which means redesigning architectures so compute and storage are separated by region.

It's easier if you are building your own applications, but it's much harder to achieve with off-the-shelf SaaS products. We have strict internal controls on greenlighting a product to ensure data residency mandates are met to mitigate this risk. Though the bigger issue is proving privacy as opposed to security controls, it's really hard to demonstrate data location when operating in a wide geographical environment such as ours. These challenges, combined with strict management of regulatory compliance, can often lead to fatigue.

When viewed in its entirety, security is manageable because we've built strong foundations. Privacy is a moving target, shaped by evolving regulations, regional demands, and the lack of clarity around what "Privacy" really means in the Cloud.

Q. How do you effectively manage CSP and CSP Platforms?

We treat cloud providers as infrastructure partners and treat them as extensions of our data center. Though this partnership model can be much tougher to implement, it can really scale well and gives us the freedom to build differentiated solutions.

CSPM tools are fairly uniform across providers, so you're not locked into using the native security tools from each Cloud. You can go with a central solution that monitors across environments. Some vendors are now offering "single pane of glass" solutions that integrate with multiple tools: CSPM, SSPM, identity, vulnerability management and give you one dashboard. They don't do security themselves but connect everything through APIs. It's a smart workaround to a growing problem.

While SaaS Security Posture Management (SSPM) is also evolving, we are also witnessing top SSPM tools struggle because every SaaS provider now wants to sell their own security module and wants to vertically integrate to provide holistic solutions. It works if you are in a single CSP environment, but not if your landscape spans across multiple clouds.

SaaS adoption will keep rising because it's efficient and fast to deploy, plus there is an obvious advantage of a faster go-to-market. However, things can be extremely challenging in the case of a security incident since troubleshooting in SaaS environments is tough, and you need to depend on the CSP for a faster turnaround time. For non-critical services, SaaS works well, but for core systems like banking, it's risky unless you've got strong reliability planning and the provider has solid regional infrastructure.

Q. What are your thoughts on looking forward to Cloud?

Cloud adoption is going to keep growing for at least the next three years. There might be a plateau as companies mature and reassess their strategies. With Amazon entering the market recently and Google announcing a data centre, competition will eventually drive prices down through achieving economies of scale.

AI is another big driver, and even large banks like ours cannot afford the infrastructure needed to run advanced AI in-house. Cloud makes it accessible through subscription models, which is far more practical, where you get to test and scale without a massive upfront investment.

SaaS, though, might see some pushback as vendor lock-in and rising costs are becoming real concerns. As hyperscale cloud adoption grows in the UAE and other GCC countries, SaaS might slow down as companies look towards more flexibility.

Commercially and scalability-wise, cloud still makes sense as on-premises costs escalate with time, whether due to licenses, hardware refreshes, or maintenance. When your strategic plan is over 10 years, the Cloud will often come out ahead.

NITIN SHINGARI

Director - Cybersecurity

Large UAE-Based Holding Company

> While cloud has truly been a disruptor, I believe the AI disruption, combined with the scalability power of cloud, will lead to further innovations and use cases.

Q. Where are you currently in your cloud journey?

With a goal of **100%** cloud native in the near future, about **50%** of our current workloads are already migrated to the Cloud. We genuinely believe that Cloud offers tremendous benefits in scalability and growth of our organization, and we consistently work on taking this strategy to a success. At present, we intend to continue our migration with a single strategic Cloud Service Provider to fully leverage the security and integration benefits that are offered.

As a holding company, our key business drivers for cloud adoption have been speed of migration, compliance with regulations, data sovereignty, cost-effectiveness and being a holistic, one-stop shop.

At the center of our strategy lies the integration principles and security by design principles. In integration, we focus on migration as integrated as possible to fully reap the benefits offered by the CSP. Keeping security by design principles during cloud adoption was guided by best practices such as the NIST Cybersecurity Framework and ISO 27001, with the security team developing a tailored set of controls for the Azure environment.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

I think one of the earliest challenges we faced was a lack of comprehensive and intuitive literature /documentation that could provide step-by-step guidance when securing the Cloud. This challenge got enhanced when we were trying to link existing security controls/ tools configurations to specific compliances like UAE IA, ISO 27001 or NIST CSF.

The next challenge is more recent, however, as we have recently been rebranded, changing the tenant's name in the CSP was not possible, and we had to migrate from scratch, causing severe operational pain and unnecessary efforts.

As an early adopter, I recommend fellow security leaders to consider the following:

- Due Diligence and preparation goes a long way.
- Performing Organizational change and internal readiness will set a foundation for a successful migration,
- Every cloud environment is unique, start with identification of control areas and available technologies and build your own custom security framework aligned with required national regulations and,
- Balance policy enrollment with business impact by designing integrated security architecture and transparent, non-intrusive policies.

Q. How do you balance security and privacy in a hybrid environment?

The trust with a CSP is the starting point since the CSP is going to act as a strategic partner for the technological scalability of the organization. This includes ensuring the CSP is not only based in the UAE but also recommended by the respective regulators. Though you may be outsourcing your computation power to a CSP, the overall risk of security still lies with the organization.

Conducting thorough assessments of the CSP before onboarding helps establish a relationship of trust. Hence, we perform screening checks and compliance assessments (SOC 2, ISO 27001, Compliance with UAE regulations, etc.) to evaluate any new CSP that is onboarded in our environment.

On-premises, the environment is stable, and we continue to follow UAE regulations. For the Cloud, compliance depends on the CSP, and we add extra due diligence, such as checking for integration with our SoC, configuration guidelines, and leveraging other security features available.

SaaS, however, needs the most scrutiny as we do not always know how and where our data is stored, or which AI models are integrated and whether our data is being used for training AI models. By running our customized privacy and security assessments before onboarding SaaS applications, we get some reasonable assurance.

At present, Identity and Access management remains a challenge as no single CSP can cover the entire technology landscape. The preliminary phase is to discover distinct roles and applications, to define the SoD (Segregation of Duties) and parallelly select an Identity and Access (IAC) process and tool which can be integrated with our JML (Joiner-Mover-Leaver) process using rule-based access controls. Since visibility is key, we rely on third-party tools to get clear insight into identity and access management in the Cloud. We also mandate MFA and SSO implementation from the secured architecture and Zero Trust Principles perspective, especially for privileged access through our IAM and PAM solutions.

Protecting data in a hybrid environment remains one of the biggest challenges, as you often require two solutions to manage the hybrid environment in the interim. Managing unstructured data in the Cloud has proven to be relatively easier to implement due to the presence of corporate data like emails, files and chats being on the Cloud as compared to the classification of structured data, which still needs the traditional approach to tackle holistic data security.

Q. How do you effectively manage CSP and CSP Platforms?

As part of the strategic relationship with the CSP, it is important to be updated on the new features being announced that can be leveraged. Often, these new features can save organizations tremendous investments in procuring separate security solutions. Post CSPs onboarding, we have multiple alignment discussions with the business and technical teams involved for alignment on how to perform the server onboarding, configuration changes and decommissioning, etc. This is closely followed by the critical element of support and knowledge transfer to fill the ever-expanding knowledge gap in security and cloud skills.

As the next step, we start implementing controls for monitoring of asset deployment, configuration, and network traffic. We define and approve appropriate tools and endpoints to curb the CSP from having unrestricted access. We also use CSP's native security tools like CSPM, SIEM, CNAP, etc., to increase our visibility and monitoring and improve our incident response time.

All larger CSPs today offer a plethora of security solutions, which should be leveraged to increase your visibility into the Cloud, and the CSP relation is at the center of this consistency.

Q. What are your thoughts on looking forward to Cloud?

Before we look ahead, it is important to recognize that Zero Trust Network Architecture (ZTNA) will remain extremely relevant when designing and securing your workloads in the Cloud. Looking ahead, I think data, identity and privacy aspects in security will play a major role for security leaders in the UAE, especially Bring your own Identity (BYOI) could become a prominent business need in the coming future to better support business requirements.

Also, as AI gets inculcated in the cloud offerings, transparency from CSPs becomes a topic of critical importance that must be addressed in the future.

ABHINAV KUMAR
AVP – Information Security
NMC Healthcare

> Empower your employees with necessary information to equip them to perform informed decisions and make them an integral part of cybersecurity strategies.

Q. Where are you currently in your cloud journey?

Considering the ever-evolving healthcare sector, with the adoption of new technology on a day-to-day basis to enhance patient care and experience, we have seen a significant jump in the adoption of cloud technologies within healthcare in recent times. As of now, **35%** of our IT workloads run in the Cloud, with the remainder still on premises. We primarily operate in a Hybrid Cloud model, with select use of multi-cloud for resilience and vendor diversification. Our cloud adoption is driven by patient care, patient experience, scalability, operational efficiency, and regulatory requirements. Key drivers also include business continuity, digital transformation, and enhanced data analytics capabilities, which assist us in delivering tailored patient care. Our strategy is aligned with security and compliance frameworks such as ADHICS, Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL), ADGM Data Protection Regulations 2021, ISO 27001, PCI DSS, and SOC 2 Type 2. Further, we keep adding more regional and global regulations and accreditations to this list, depending on the cloud provider in mind.

Q. What have been the top learnings and challenges? What would be your advice to fellow security leaders embarking on this journey?

Our venturing into the cloud journey presented significant challenges, primarily due to legacy system integration, data sovereignty concerns, and a lack of visibility across IT and IoMT environments. A major challenge involved unauthorized access attempts on misconfigured cloud workloads, which we swiftly mitigated through enhanced access management, continuous posture assessments, and the deployment of a centralized SIEM and SOAR for visibility into real-time threat response.

Key lessons learned primarily include the criticality of shared responsibility awareness among end users and IT, securing cloud-native configurations from day one through an integrated security by design, and embedding DevSecOps early in cloud adoption. Continuous monitoring and regular red teaming activities have also been instrumental in identifying evolving attack vectors.

My primary advice to other CISOs/CIOs is to stop considering humans as the weakest link in the cybersecurity chain and look towards implementing preventive controls that provide necessary information to humans so that they can be enabled to make informed decisions and assist us in implementing complex cybersecurity strategies. In addition to this, we should always treat the cloud environment like an extension of our enterprise and not as a separate environment. Prioritize visibility, automate controls, adopt zero-trust, and invest in cloud-native security tools. Equally important is staff training and securing third-party integrations. A proactive and well-governed cloud strategy is vital for resilient healthcare IT / IoMT operations.

Q. How do you balance security and privacy in a hybrid environment?

Managing cybersecurity in a multi-cloud and hybrid environment requires a unified approach to be created before the CSP is onboarded and the migration is initiated. We have implemented a **centralized data classification and protection framework** applicable across on-prem and Cloud, aligned with UAE regulatory requirements like **ADHICS and PDPL**. We also use **automated discovery tools** to classify and label sensitive data, particularly PHI/PII, due to the critical nature of our business. However, the key challenge has been the **inconsistent security controls between platforms and legacy medical devices**, which creates **limited visibility** during integration. We also adopted cloud-native security tools to enhance visibility, integrated our SIEM with the cloud infrastructure, and added multi-layered cybersecurity controls with conditional access and MFA to address this. Collaboration between security, compliance, End users and IT teams has been critical for successfully adopting a multi-cloud environment. It has enabled us to truly reap the benefits of a successful cloud migration.

Q. How do you effectively manage CSP and CSP Platforms?

We manage Cloud Service Providers (CSPs) as an integral part of our cybersecurity and risk governance framework. We follow a structured **vendor risk management process**, which includes **security due diligence, data protection impact assessments,** and **contractual enforcement of compliance with ADHICS, UAE PDPL, ADGM Cybersecurity Framework and ISO 27001 standards**.

Before onboarding any CSP, we carefully assess their **security certifications (e.g., SOC 2, ISO 27017), data residency practices**, and their ability to support **multi-tenancy isolation** and **zero trust architecture**.

Once onboarded, we also maintain visibility through **Cloud Security Posture Management (CSPM) tools** integrated into our **SIEM (Securonix)**, allowing us to monitor misconfigurations and ensure continuous compliance. We also leverage **native CSP tools like AWS Security Hub and Azure Defender**, along with periodic **security assessments** and **third-party audits**. We allow administrative access to our vendor on our cloud environment through PAM only, and we review all PAM logs periodically for consistent identification of potential security incidents.

Our approach ensures CSP alignment with our broader cyber resilience strategy while protecting patient data and maintaining regulatory readiness.

Q. What are your thoughts on looking forward to Cloud?

From a cybersecurity perspective, the biggest threats to cloud adoption in the next 3–5 years include misconfigured services, the compromise of legacy systems through the supply chain, and evolving AI-driven attacks.

AI and automation will play a critical role in threat detection, response, and predictive risk analytics, enhancing both speed and accuracy. Looking ahead, strengthening cloud security will be paramount. We are investing in unified security platforms, AI-enabled threat detection, and continuous cloud configuration monitoring to try to mitigate upcoming potential risks.

We anticipate a significant shift toward autonomous cloud security frameworks, where AI detects and auto-remediates threats with minimal human intervention, improving resilience across complex cloud ecosystems.

What Leaders See Coming?

Two threat vectors define the risk horizon. AI-driven attacks represent a qualitative shift in adversary capability, not incremental evolution. The UAE Cybersecurity Council foiled AI-powered attacks on vital national sectors in early 2026, and several leaders interviewed for this whitepaper cited AI-augmented identity exploitation as their most pressing near-term concern.

Supply chain risk is the second frontier. As UAE organisations deepen integrations with SaaS platforms, third-party APIs, and managed service providers, the attack surface extends well beyond what any single organisation controls. IBM found that **40%** of breaches globally involved data across multiple environments, leading to an avergae cost of data breach to be around $5M. Third-party due diligence and continuous supply chain visibility are operational necessities, not compliance checkboxes.

90,000-200,000

breach attempts targeting the UAE every single day - many state-sponsored

Source – The National News, UAE foils AI-powered 'terrorist cyber attacks' on vital sectors, Feb 2026.

~$5M

avg. cost of a databreach globally

Source – IBM Cost of Data Breach Report 2024.

Key Leadership Summary

Five Strategic Priorities for Securing the Cloud in the UAE

01. AI Security & Governance

AI workloads are rapidly driving cloud adoption, but also brings forth new governance, privacy, and security challenges that organizations must address.

02. Identity, Zero Trust, Data Security & Privacy

As perimeters dissolve, organizations are adopting identity-centric Zero Trust architectures, enforcing least-privilege access and MFA, and embedding data privacy controls across hybrid and multi-cloud environments – with IaC increasingly becoming the de-facto mechanism of consistent controls implementation.

03. Visibility & Cloud Security Operations

Maintaining real-time visibility, enforcing the shared responsibility model, and managing CSPM, SIEM/SOAR, and threat detection across multi-cloud estates remain critical operational priorities.

04. Governance, Compliance & Vendor Risk

Regulatory compliance, data residency requirements, and SaaS security risks significantly influence cloud adoption strategies, particularly in regulated sectors such as government, banking and critical infrastructure. Strategic partnerships with CSPs are critical via shared responsibility, contractual governance and technical validation.

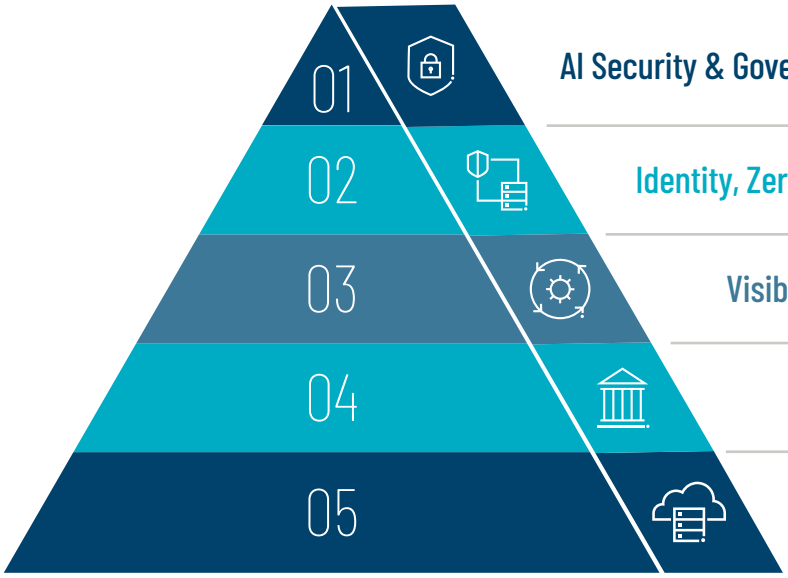
05. Cloud as the Digital Foundation

Cloud adoption across the UAE is now the strategic digital backbone — for most enterprises, over half of their technology footprint already resides in the cloud. Sustaining this transformation demands alignment across people, process, and technology: cultivating a culture of security through continuous awareness and training; embedding financial discipline and risk-based governance into cloud processes; and building technology foundations designed for resilience and innovation from the outset.

protiviti®

Protiviti's Cloud Security Transformation Pyramid

A pragmatic, layered approach to securing cloud environments — building resilience from the ground up



AI Security & Governance

Identity, Zero Trust, Data Security & Privacy

Visibility & Cloud Security Operations

Governance, Compliance & Vendor Risk

Cloud as the Digital Foundation

01 AI Security & Governance

- AI/ML model risk
- LLM security
- AI governance frameworks

Assess model risk, defend against LLM vulnerabilities, and govern the deployment of generative AI responsibly.

Where to start - DESC AI Security Policy + CSA AI Safety Initiative

02 Identity, Zero Trust, Data Security & Privacy

- IAM & PAM
- Zero Trust architecture
- MFA & JML lifecycle
- Data Security & Privacy controls

Enforce least-privilege access, implement Zero Trust architectures, manage cloud identity lifecycles end-to-end, and embed data privacy controls.

Where to start - NIST SP 800-207 (Zero Trust Architecture)

03 Visibility & Cloud Security Operations

- CSPM & CNAPP
- SIEM / SOAR
- Multi-cloud threat detection

Maintain real-time visibility across multi-cloud estates through posture management, SIEM/SOAR, and automated threat response.

Where to start - MITRE ATT&CK Cloud Matrix

04 Governance, Compliance & Vendor Risk

- NCSP, DESC, ADHICS, PDPL
- Data sovereignty
- CSP risk management

Align with UAE regulations, enforce data residency controls, and manage third-party cloud provider risk across the supply chain.

Where to start - NCSP controls mapping to ISO 27017

05 Cloud as the Digital Foundation

- Cloud-first strategy
- Shared responsibility model
- Secure landing zones

Establish secure, governance-ready cloud environments from day one clarifying shared responsibility and enabling safe innovation at scale.

Where to start - CIS Benchmarks for your CSP

Appendices

Appendices: Supporting the Conversation

Glossary of terms

- **ADGM** *Abu Dhabi Global Market*
- **ADHICS** *Abu Dhabi Healthcare Information & Cybersecurity Standard*
- **AI** *Artificial Intelligence*
- **AUS** *American University of Sharjah*
- **AWS** *Amazon Web Services*
- **BYOI** *Bring Your Own Identity*
- **CAGR** *Compound Annual Growth Rate*
- **CAPEX** *Capital Expenditure*
- **CASB** *Cloud Access Security Broker*
- **CI/CD** *Continuous Integration and Continuous Deployment*
- **CIO** *Chief Information Officer*
- **CISO** *Chief Information Security Officer*
- **CNAPP** *Cloud Native Application Protection Platform*
- **CSF** *Cybersecurity Framework*
- **CSPM** *Cloud Security Posture Management*
- **CSPs** *Cloud Service Providers*
- **CSA CCM** *Cloud Security Alliance's Cloud Controls Matrix*
- **CWPP** *Cloud Workload Protection Platform*
- **DESC** *Dubai Electronic Security Center*
- **DevSecOps** *Development, Security, and Operations*
- **DOH** *Department of Health*
- **EPSS** *Exploit Prediction Scoring System*
- **GCC** *Gulf Cooperation Council*
- **GCP** *Google Cloud Platform*
- **GDPR** *General Data Protection Regulation*
- **HECVAT** *Higher Education Community Vendor Assessment Toolkit*
- **IaC** *Infrastructure as Code*
- **IAM** *Identity and Access Management*
- **IaaS** *Infrastructure as a Service*
- **IDC** *International Data Corporation*
- **IDS** *Intrusion Detection Systems*
- **IoMT** *Internet of Medical Things*
- **IPS** *Intrusion Prevention System*
- **ISO** *International Organization of Standardization*
- **IT** *Information Technology*
- **JML** *Joiner-Mover-Leaver*
- **KSA** *Kingdom of Saudi Arabia*
- **MCAF** *Minimum Cybersecurity Assurance Framework*
- **MFA** *Multi Factor Authentication*
- **MITRE ATT&CK** *MITRE Adversarial Tactics, Techniques, and Common Knowledge*
- **ML** *Machine Learning*
- **NCSP** *National Cloud Security Policy*
- **NIST** *National Institute of Standards and Technology*
- **OCI** *Oracle Cloud Infrastructure*
- **OPEX** *Operational Expenditure*
- **PaaS** *Platform as a Service*
- **PAM** *Privileged Access Management*
- **PDPL** *Personal Data Protection Law*
- **PIM** *Privileged Identity Management*
- **RBAC** *Role-Based Access Control*
- **SaaS** *Software as a Service*
- **SASE** *Secure Access Service Edge*
- **SIEM** *Security Information and Event Management*
- **SOAR** *Security Orchestration Automation and Response*
- **SOC** *Security Operation Center*
- **SoD** *Segregation of Duties*
- **SP** *Special Publication*
- **SSO** *Single Sign-On*
- **SSPM** *SaaS Security Posture Management*
- **SSRM** *Shared Security Responsibility Model*
- **UAE** *United Arab Emirates*
- **UAE IAS** *UAE Information Assurance Standard*
- **XDR** *Extended Detection and Response*
- **ZTINA** *Zero Trust Network Architecture*

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Contacts

Niraj Mathur
Managing Director
+971 502547507
Niraj.Mathur@protivitiglobal.me

Varun Kukreja
Senior Director
+971 502926071
Varun.Kukreja@protivitiglobal.me

Acknowledgement

Sinduja Sridhar, **Karan Arora**, & **Niloufar Kianfar** from our Technology & Digital team have contributed to this publication.

Our Offices in the MENA

Abu Dhabi
Emirates Real Estate Corporation
Building, 7th Floor, Office 707-711
Al Falah Street, Al Danah,
P.O. Box 32468, Abu Dhabi, UAE

Bahrain
Platinum Tower, 17th Floor
P.O. Box 10231, Diplomatic Area
Manama, Kingdom of Bahrain

Dubai
Office No. 2104, 21st Floor
U-Bora Tower 2, Business Bay
P.O. Box 78475, Dubai, UAE

Egypt
Cairo Complex
Ankara Street Bureau 1
First Floor, Sheraton Area
Heliopolis - Cairo, Egypt

Kuwait
Al Shaheed Tower, 4th Floor
Khaled Ben Al Waleed Street, Sharq
P.O. Box 1773, Safat 13018, Kuwait

Oman
Al-Ufuq Building, 2nd Floor
Office No. 26, Shatti Al Qurum
P.O. Box 1130, P.C. 112
Ruwi Muscat, Oman

Qatar
Palm Tower B 19th Floor
P.O. Box 13374, West Bay
Doha, Qatar

Saudi Arabia - Dammam
Q1-5, The Business Quarter
Salman Al Farisi St,
Al Khalidiyyah Al Janubiyyah,
Dammam, Eastern Province, 32221,
Kingdom of Saudi Arabia

Saudi Arabia - Jeddah
King Abdulaziz Branch Road
Ash shati district, Building No. 7524
P.O. Box 3675, Jeddah 23412
Kingdom of Saudi Arabia

Saudi Arabia - Riyadh
Al-Ibdaa Tower, 9th & 18th Floor
King Fahad Branch Road, Al-Olaya,
Building No. 7906, P.O. Box 3825
Riyadh 12313, Kingdom of Saudi Arabia

Face the Future with Confidence®

157846_OCT2025