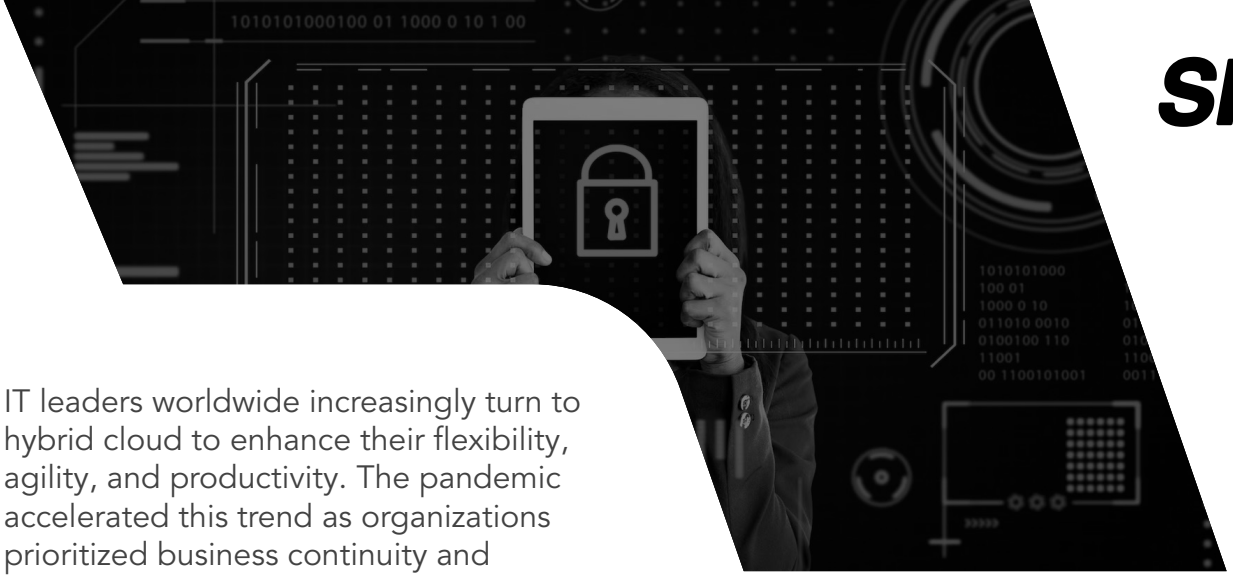
SISA

DATA SECURITY CHALLENGES IN HYBRID CLOUD AND SIX BEST PRACTICES TO OVERCOME THEM



IT leaders worldwide increasingly turn to hybrid cloud to enhance their flexibility, agility, and productivity. The pandemic accelerated this trend as organizations prioritized business continuity and flexibility, leading to accelerated adoption of hybrid cloud. According to a report by Cisco[1], 82% of IT leaders have adopted the hybrid cloud model. However, deploying a hybrid cloud presents several challenges, with data security being the most significant. Over one-third (37%) of IT professionals consider security the primary challenge when deploying a hybrid cloud[2]. The rapid adoption of hybrid cloud has also led to a rise in data breaches, with banking, fintech, and payments firms being prime targets. This has spotlighted data security, especially for regulated sectors with a high risk of sensitive data loss.

Navigating a challenging landscape

Developing an effective **data protection** strategy is one of the biggest challenges for businesses that want to leverage the benefits of a hybrid cloud, particularly when working across multiple platforms and locations. This challenge is further compounded by various operational, administrative, and technical issues plaguing cloud environments. These issues include:

Figure 1: Top 5 challenges of hybrid cloud model

Proliferation of cloud databases

Hybrid clouds combine cloud and on-premises data storage servers, each with its own security protocols and guidelines. In the financial services sector, regulatory requirements may differ between each environment, making it a daunting task to plan for storage and access requirements. Achieving this requires investments in specialized IT personnel, tools, resources, and employee training.

Lack of visibility and control

Enterprise admins have long been concerned about gaining visibility and control across distributed systems. The mix of public and private clouds can increase system complexity and risks, resulting in a lack of accountability.

> **Organizations face two common challenges: unsanctioned app use, also known as shadow IT, where employees use applications not permitted by IT, and sanctioned app use, where IT-approved apps are not used as intended.**

These challenges can undermine system security and increase organizational risk, making it imperative for businesses to implement strategies to mitigate these issues.

Difficulty in governance and monitoring

Each public and private cloud service has its own unique security and privacy requirements, and transferring data between them can result in a loss of visibility and control. One of the major challenges is clearly defining security governance responsibilities between the in-house team and the cloud provider. Additionally, monitoring tools that come with cloud services are often incompatible with existing solutions, presenting integration challenges. Furthermore, using these tools typically requires accessing cloud dashboards that are difficult to use and may potentially delay the detection and reporting of incidents. As a result, it's important for organizations to carefully evaluate their security needs and select cloud services and tools that align with their security goals and enable seamless integration.

The gap in knowledge and skills

Finding professionals with the necessary skills is a significant challenge for organizations implementing hybrid cloud. An IDC survey[3] found that more than 70% of respondents reported a cloud skills gap in their organizations. The pandemic-induced wave of cloud adoption has only exacerbated the talent crisis. This skills gap has a profound impact on organizations' ability to perform effectively while exposing them to significant security risks. Addressing the skills gap requires investing in employee training and development, partnering with cloud service providers, and working to attract and retain skilled professionals. Failure to address the cloud skills gap can impede organizational growth and hinder the ability to leverage the full potential of the hybrid cloud.

Difficulty in identifying unstructured data

Data discovery and classification, especially within unstructured data, is a major challenge for many organizations. Unstructured data represents a staggering 80% of all new enterprise data, according to Gartner estimates, and it's growing three times faster than structured data[4].

> **Traditional on-premises tools and data loss prevention methods are geared toward protecting on-premise data and are not designed for cloud storage, making tracking, accessing, and governing such data difficult.**

Furthermore, organizations are grappling with the rise of shadow data - data that is not available or subject to an organization's centralized data management framework - posing a significant challenge to data security and compliance. To address these challenges, organizations need to invest in tools and strategies designed specifically for cloud storage, prioritize data discovery and classification, and implement robust data management frameworks that address the complexities of both structured and unstructured data. Failure to address these issues can lead to data breaches, compliance violations, and reputational damage.

Threat vectors in a hybrid cloud

The widespread adoption of hybrid cloud has increased the attack surface for organizations, making stronger controls and enhanced cyber defenses essential. With a constantly evolving threat landscape, organizations must contend with new and emerging risks, adding complexity to the hybrid cloud environment. The leading security risks and threat vectors associated with hybrid cloud are discussed below.

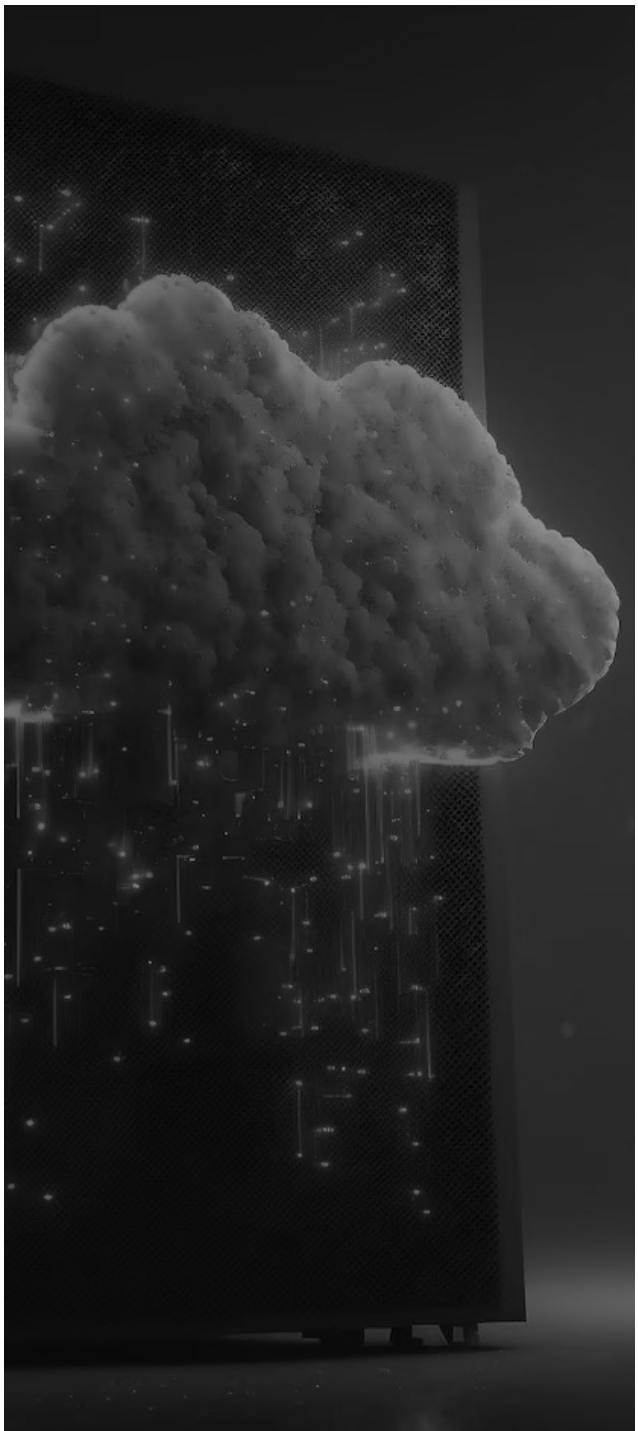
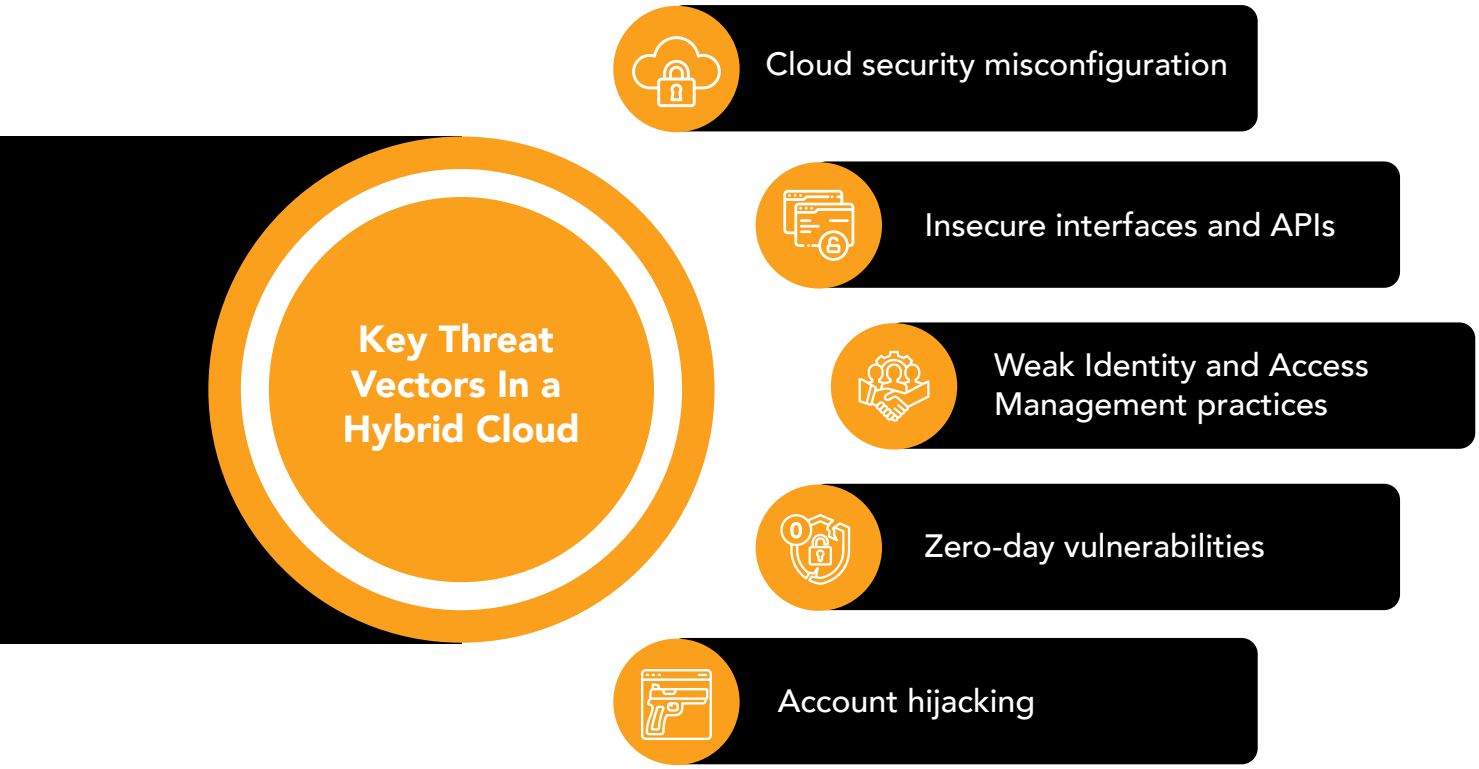


Figure 2: Key threat vectors in hybrid cloud



Cloud security misconfiguration

A cloud security misconfiguration occurs when a cloud resource is incorrectly configured, leaving data and systems vulnerable to attack. Misconfigurations can happen at any stage of the cloud computing lifecycle and are typically caused by human error, default configurations, architectural design issues, and a lack of understanding of security services. Insecure storage, excessive permissions, default credentials, and ineffective change control can also lead to vulnerabilities.

Insecure interfaces and APIs

Cloud APIs and user interfaces are highly exposed components of a cloud environment and have become prime targets for hackers. API attacks experienced a staggering 168.8% increase in the first half of 2022 compared to the same period in 2021[5]. Roughly 5 billion (31%) of the 16.7 billion malicious requests observed targeted unknown, unmanaged, and unprotected APIs, also known as shadow APIs[6]. This makes shadow APIs the top threat facing cloud environments.

> **SISA's findings in the Top 5 Forensic-driven Learnings Report also reveal that there has been a 37% increase in intruders exploiting unknown web interfaces and API calls that information security teams were unaware and for which they had not deployed controls.[7]**

Weak Identity and Access Management practices

Ineffective and weak Identity and Access Management (IAM) practices present a significant cloud security challenge. Cloud infrastructure requires a sophisticated system of granular control because users access resources primarily at the application or modular level. However, a majority of cybersecurity threats, including those related to the cloud, can be traced back to IAM issues, particularly those caused by inadequate credential protection, lack of automated cryptographic key, password and certificate rotation, weak passwords, and absence of multi-factor authentication (MFA). Findings from SISA's forensic investigations reveal that the compromise of cloud account credentials and the absence of MFA is a common ingress point for intruders to access cloud environments. As a result, businesses must prioritize IAM strategies that are robust, secure, and efficient, including MFA, automated key rotation, and strong password policies. This is critical for protecting cloud infrastructure from security breaches and ensuring that sensitive data remains secure.

Zero-day vulnerabilities

Many hybrid cloud environments prioritize perimeter security while ignoring in-depth defenses, leading to weak network segmentation and opening the door to attackers and malware. The increased use of open-source software and public cloud also makes it nearly impossible for any known vulnerability to go unexploited, creating ample opportunities for hackers to launch zero-day attacks that target newly identified vulnerabilities before they're patched.

This leaves system administrators and developers with a limited window of opportunity to perform necessary software updates and maintenance before vulnerabilities are exploited.

> **SISA has observed a trend of hackers targeting vulnerable applications, such as UAT systems and non-critical applications with web interfaces, and deploying backdoors in servers to access sensitive IT data and assets.**

Common vulnerabilities that are exploited include SQL injection, malicious file upload, OS command injection, and security misconfigurations. To prevent these attacks, organizations need to prioritize in-depth defenses and security measures, including proactive vulnerability management, threat monitoring, and regular software updates and maintenance. This is critical for protecting sensitive data and assets from potential breaches and attacks in hybrid cloud environments.

Account hijacking

Account hijacking, also known as account takeover, is a serious cloud security threat that involves the disclosure, leakage, exposure, or compromise of critical cloud accounts. Hackers use various tactics, such as phishing, keylogging, cross-site scripting attacks, and brute force attacks, to steal user account credentials, potentially leading to data breaches and service disruptions. Financial service providers, including banks and insurers, are common targets for account hijacking due to the lure of financial gain or identity theft for money laundering.

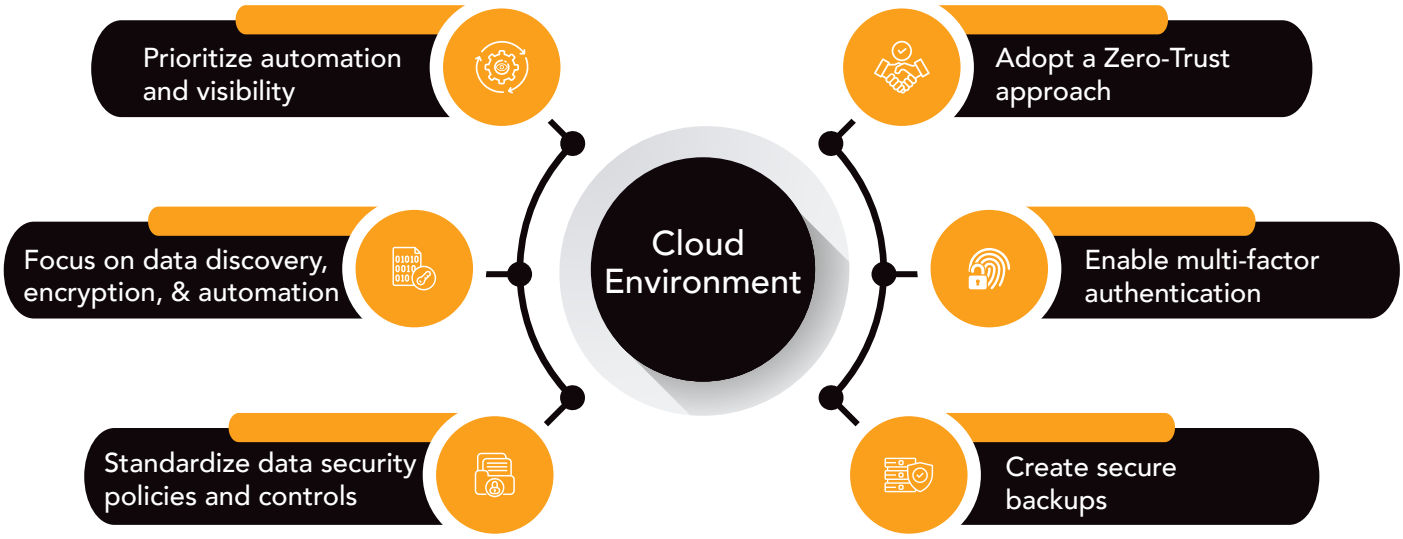
> **Account takeover attacks increased by a staggering 131% in the first half of 2022 compared to the same period in 2021[8], highlighting the growing security risk to cloud environments.**

To mitigate this risk, organizations need to prioritize security measures such as strong authentication methods, employee training on identifying and preventing phishing attacks, and monitoring for suspicious activity in cloud accounts. This is critical for protecting sensitive data and ensuring business continuity.

Best practices for securing sensitive data

As businesses increasingly turn to hybrid cloud environments to take advantage of the benefits of both on-premises and cloud-based data storage, it's critical to prioritize security best practices to keep data safe and secure. Organizations must consider the following best practices to help them secure their cloud programs.

Figure 3: Best practices for securing sensitive data in hybrid cloud



Prioritize automation and visibility

To secure your data in hybrid cloud environments, the first step is gaining complete visibility. This enhanced visibility enables organizations to identify potential issues before they become problems and pinpoint unused apps, access points, and other resources that may be overlooked. Adopting cloud automation to automate repetitive tasks such as producing logs, ingesting data, provisioning workloads, and managing and monitoring system performance can improve visibility and reduce the risk of human error.

Best practice

Automate monitoring and risk assessment with defined access and usage rules for hybrid environments.

Focus on data discovery, encryption, and automation

Regularly identifying and classifying sensitive and regulated data across private and public cloud environments is critical for maintaining a secure hybrid cloud environment. Implementing an integrated **data discovery and classification solution** should be a top priority, as it helps identify the location, exposure, and spread of sensitive data. Secondly, all sensitive data must be encrypted at rest and in transit. Additionally, organizations must consider using cryptographic protocols (SSL/TSL) for secure transmission over the network.

Best practice

Implement a robust data discovery solution and automate remediation workflows to reduce sensitive data exposure.

Standardize data security policies and controls

Effective security controls are critical to securing sensitive data in hybrid cloud environments. However, different cloud services may require different security controls and solutions. It is important to define and implement consistent security controls as close to the data storage location as possible at the lowest practical level. Secondly, defining and assigning data protection policies, regularly educating the users about these policies and enforcing data sharing policies for each cloud service are critical steps for securing sensitive data.

Best practice

Conduct regular audits to standardize data security policies across all cloud services.

Adopt a Zero-Trust approach

Zero trust is a popular security approach that verifies every user's access based on multiple factors. This approach can flag suspicious activity and revoke access.

> **Zero Trust Network Access (ZTNA) architecture brings disparate infrastructure under a secure access point, by implementing strong IAM policies, assigning role-based access and exercising the principle of least privilege.**

These controls can reduce possible threat profiles in the event of an account compromise or misuse.

Best practice

Implement granular IAM policies and the principle of least privilege to define user access.

Enable multi-factor authentication

Multi-factor authentication (MFA) is crucial for ensuring authorized access to sensitive payment data, particularly in the payments and financial industry, where data security is paramount. By combining factors such as passwords and biometrics, MFA can provide an extra layer of protection against unauthorized access.

> **For maximum effectiveness, MFA should be applied consistently across all applications and system components and should be implemented as out-of-band authentication.**

Best practice

Implement adaptive MFA with single sign-on (SSO) and least privilege access.

Create secure backups

To ensure recoverability in case of data loss, organizations must backup both cloud-based and on-premises data, while keeping backup storage distinct from the original data source. Following the 3:2:1 rule of creating three copies of data on two storage media with one offline copy is highly recommended. The practice of using WORM copies – write once and read many times, implementing retention policies, encrypting backups, using immutable backup copies, and restricting hosts/IP access for added security are other standard best practices to secure backups.

Best practice

Secure hybrid cloud backups by implementing strong retention policies, encrypting backups, and using immutable copies

Conclusion

A hybrid cloud is becoming a reality for many CIOs despite the security risks and operational challenges. In 2023 and beyond, enterprises will optimize their hybrid environments with a defined business and technology strategy, including data synchronization, governance, disaster recovery, and cost management across both systems. As third and fourth-party dependencies in cloud services expand, the importance of a holistic approach to security will only grow stronger, requiring end-to-end risk management and mitigation. To address the talent shortage and accelerate digital-first strategies, enterprises and service providers will set up data security centers of excellence, serving as a centralized hub for orchestrating enterprise-wide data security strategy.

How SISA Radar can help secure sensitive data on cloud

SISA Radar – SISA's Data Discovery and Classification tool helps address the data protection challenges of enterprises with data discovery, file analysis, and data classification. It offers a single platform to automate the discovery process, identify sensitive data, and contextualize data for users. By leveraging artificial intelligence and machine learning, SISA Radar is able to identify data assets and processes that have a high risk of exposure – helping organizations mitigate risks. Learn how SISA Radar helped a **leading fintech in APAC** streamline sensitive data discovery and classification to achieve compliance and how an **American healthcare MNC** strengthened its data security policy by integrating SISA Radar with DLP solutions.

References

1. https://www.techrepublic.com/article/report-82-of-it-leaders-are-adopting-the-hybrid-cloud/
2. https://www.techrepublic.com/article/report-82-of-it-leaders-are-adopting-the-hybrid-cloud/
3. https://www.sdxcentral.com/articles/news/the-cloud-skills-shortage-still-worries-it-leaders/2022/03/
4. https://saxon.ai/blogs/how-to-tap-the-power-of-unstructured-data-in-2022-and-beyond/
5. https://www.rtinsights.com/cyber-attacks-against-api-services-surge/
6. https://www.darkreading.com/attacks-breaches/more-than-30-of-all-malicious-attacks-target-shadow-apis
7. https://www.sisainfosec.com/infosec-reports/sisa-top-5-forensic-driven-learnings-2023-24/
8. https://venturebeat.com/security/report-account-takeover-attacks-spike-fraudsters-take-aim-at-fintech-and-crypto/

About SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

SISA is one of the leading global forensic investigators for the payments industry.

1,000+	2,000+	40+
Active engagements	Global customers served	Countries

Global Presence

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia