GBM 9th Annual Security Report 2020

GBM

A FUTURE REIMAGINED

How can Gulf Organizations transform security strategies to prepare for the next normal of digital economy

CONTENTS

FOREWORD

As technological disruption leads to rapid digitalization of the global economy, organizations have to re-imagine the architecture of the enterprise. Organizations are leveraging technology to redesign customer and employee engagement, transform operations, and adopt new business models to address rapidly changing industry dynamics and user needs.

As organizations reshape themselves to adapt to the expanding digital economy, building resilience and trust into digital experiences of customers, employees and partners is becoming increasingly critical. There is a realization now that security needs to be central to the digital architecture of the future enterprise to engender trust and resilience. However, developing a digital strategy where security is “baked in” and not “bolted on” is challenging, and requires an understanding of risks across all facets of the enterprise, and furthermore, an attention to building comprehensive security strategies to address them.

In the 9th edition of GBM Annual Security Report, we look at how risk priorities have changed this year for organizations in the Gulf, and what security strategies they are employing as they accelerate towards a digital enterprise. The report is based on a survey of organizations across key industry sectors in the United Arab Emirates, Oman, Kuwait, and Bahrain. The report analyses the key results of the survey, and furthermore, provides essential guidance to security strategists and practitioners as they strive to reimagine security for the future digital enterprise.

Hani Nofal

Hani Nofal
VP of Digital Infrastructure Solutions

GBM

INTRODUCTION

THE FUTURE OF WORK IS CHANGING AND WILL NEVER BE THE SAME ANYMORE

AS the global digital economy expands, organizations need to prepare for a future where the needs of customers, and employees will be significantly different from today. Customer needs are increasingly being shaped by Millennials and Gen Z users who are ubiquitously connected, digitally-savvy and less tolerant of complexity and latency. Members of these population segments also value individuality and personalization more than others.

These younger age groups form the majority of the population of the Middle East. In order to engage with such customers, taking a “digital – first” approach to products and services is becoming an imperative for organizations in the region. Several government organizations are accelerating the roll out of contactless services for citizens and residents and integrating them into “customer journeys” through digital platforms

Leading banks have launched “digital-only” brands and are shifting most transactions from physical branches to online and mobile channels. Traditional retailers are scaling up their ecommerce platforms and distribution capabilities in order to compete with “born-digital” online marketplaces. Educational organizations are shifting to “blended online plus offline” learning models. Healthcare organizations are increasingly providing remote services such as tele-consultation and tele-medicine services to complement on-premise services being delivered from physical health centers.

The future of work is going to be very different from the present. As the Millennials and Gen Z populations rapidly enter the workforce, workplaces and work culture are being transformed to cater to their preferences. Increasingly, enabling employees to work from anywhere, is becoming a critical capabiliy for organizations. Organizational interactions are rapidly shifting to virtual platforms, enabled by advanced collaboration technologies.

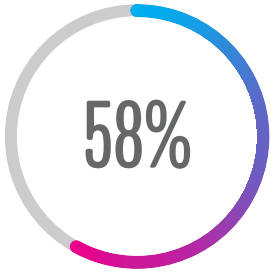
To provide rich experiences to an increasingly distributed and digitally-savvy customer and employee base, organizations are increasing their investment in applications, infrastructure and devices. Cloud is becoming the foundational model that provides the scalability and agility for the delivery of data and services. As a result, the digital surface area is expanding at an unprecedented scale, and protecting it from external and internal risks is becoming a key challenge and priority for organizations.

ACCELERATED DIGITAL TRANSFORMATION

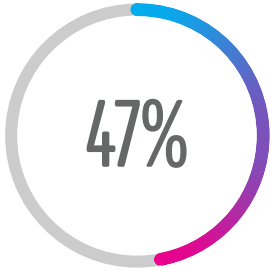
THIS year considering the focus on budget rationalization and cash preservation, we have witnessed an acceleration of digital transformation initiatives among organizations in the Gulf. As a young and tech-savvy region we have an opportunity to leverage technology to soften the impact of the economic downturn and expedite the recovery.

Digital Transformation for organizations are made up of multiple initiatives which help achieve the vision of creating digital businesses. According to IDC, 58% of organizations in the Gulf (excluding Saudi Arabia), are accelerating some of their business critical digital initiatives this year.

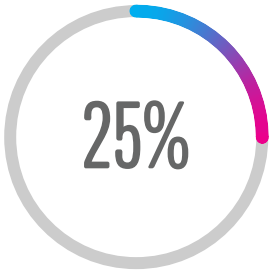
DIGITAL TRANSFORMATION TRENDS IN THE GULF 2020



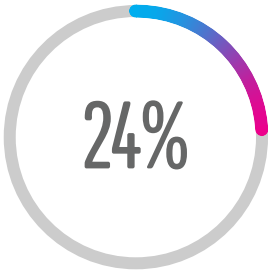
Accelerate exising digital tansformation efforts even more to meet new customer and operational agility needs



Continue with digital transformation initiatives as planned at the start of the year



Initiate completely new digital transformation efforts to meet the changed or changing customer and operational needs



Slow down or stall digital transformation efforts and focus on “keeping lights on” IT tasks

Source: IDC CIO Surveys Q2 2020; UAE, Kuwait, Oman & Bahrain; N=113

GBM

This acceleration, driven by new customer, employee and operational needs, is being enabled by 3 major technology adoption trends

Accelerated Shift to the Cloud

Unprecedented Distributed Collaboration

Application Explosion

Accelerated Shift to the Cloud

Organizations in the Gulf have fast-tracked their adoption and use of cloud this year. Spending across cloud models – private and public – has increased significantly. Most medium and large organizations are rapidly moving towards a hybrid, multi-cloud environment. The GBM survey shows that 60% of Gulf organizations have invested in cloud services in the last 6 months to support their digital initiatives. Cloud is increasingly providing the infrastructure agility, application functionality and data orchestration, that can scale up digital initiatives.

Unprecedented Distributed Collaboration

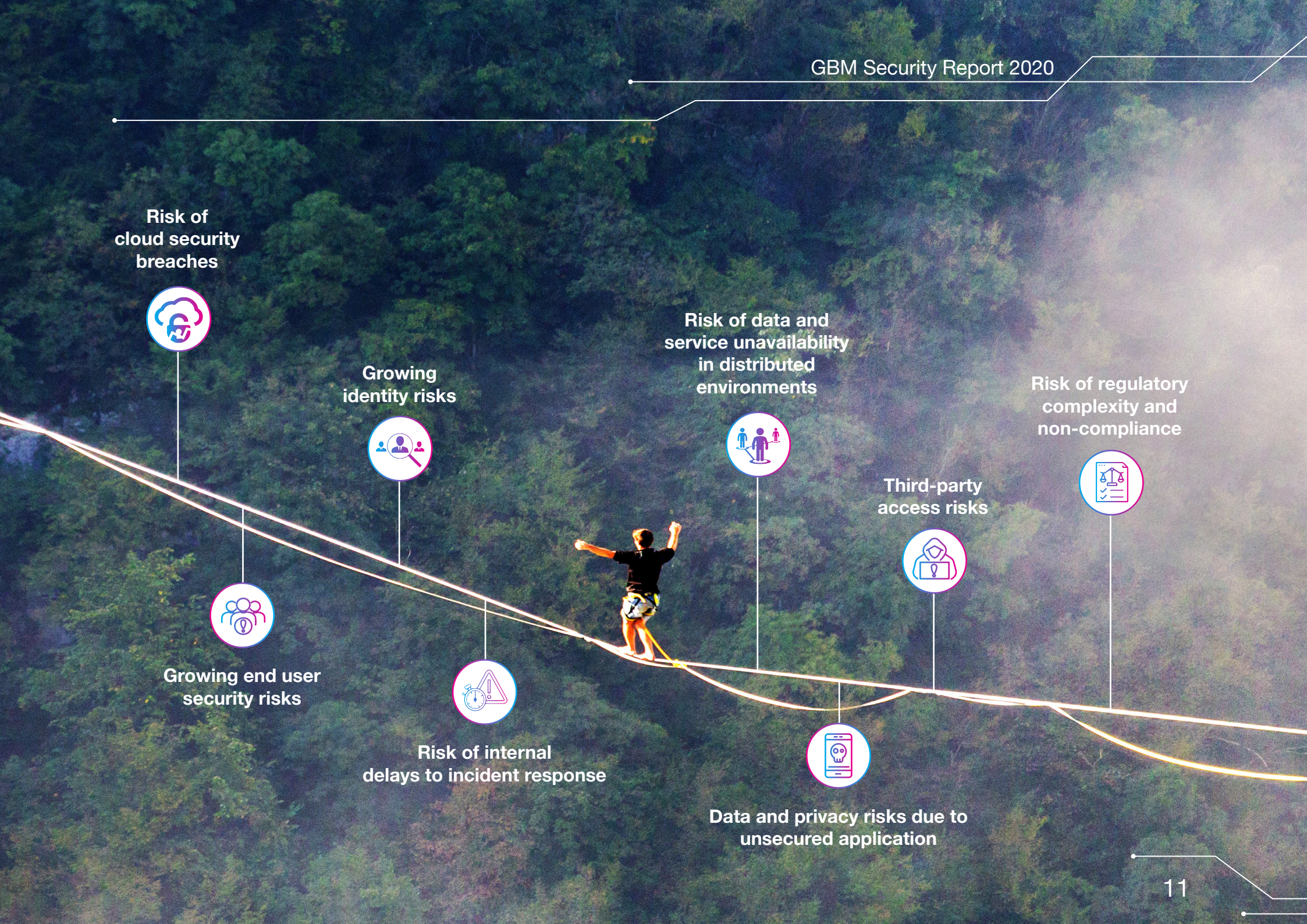
A significantly larger proportion of the workforce is working from distributed locations this year. Enabling this distributed workforce with devices and connectivity, and secure access to applications and data has become a key priority for organizations. Investment in tech-enabled collaboration has increased substantially. According to the GBM survey, 57% of the organizations are prioritizing investment in collaboration tools this year. Cloud-based collaboration platforms, that support rich interaction among distributed workers, and between employees and customers, are transforming the way work is delivered.

Application Explosion

The demand for the deployment of new applications to enable digital experiences has increased greatly this year. According to IDC, 48% of Gulf CIOs are spending more on mobile applications this year than earlier. Many of these applications are being deployed in cloud environments – which also provide easier access to distributed users. Modernization of legacy applications through containerization or refactoring into cloud-native microservices architectures has also picked up speed.

RISKS REPRIORITIZED

THE rapid shifts in technology adoption in 2020, as compared to 2019, are leading to a significant reprioritization of risks this year. This reprioritization, in turn, requires CISOs and CIOs to invest in security technologies and processes differently to ensure holistic security. The following are the key risks which radically shifted in priority when compared to 2019, that Gulf organizations are mainly concerned about.


Risk of cloud security breaches
Growing identity risks
Risk of data and service unavailability in distributed environments
Risk of regulatory complexity and non-compliance
Third-party access risks
Growing end user security risks
Risk of internal delays to incident response
Data and privacy risks due to unsecured application

Risk of cloud security breaches

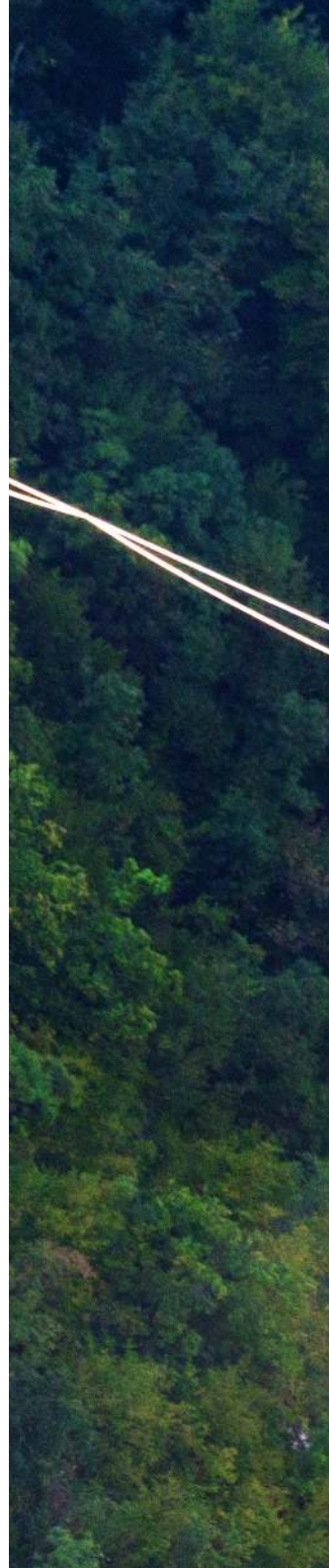
As cloud adoption greatly accelerated in 2020, managing security across a distributed, hybrid, multi-cloud environment has become a key challenge and concern. Securing applications and data in cloud environments is becoming increasingly critical. However, many organizations are unprepared – 34% of those surveyed are concerned that their cloud security measures are ineffective.

Growing end user security risks

With the expansion of the distributed workforce, protecting end users has become a key priority for organizations this year. Distributed workers often leverage unsecured home connections and personal devices, which are more vulnerable to threats than office-based systems. 84% of organizations surveyed by GBM say that this year, they are most concerned about threats such as phishing, business email compromise, and ransomware, which could make their way through unsecured end user systems.

Growing identity risks

Ensuring identity integrity and secure access to applications and data for workers is critical to delivering high levels of productivity in a distributed work environment. However, as more users are working remotely this year, 66% of surveyed organizations find that managing the identities and access of end users in multi-cloud and hybrid cloud environments is a challenge.



Risk of internal delays to incident response

Security incidents require immediate response based on collaboration among the members of the security operations team. Collaboration was relatively easier when operating out of a security operations center, however virtual collaboration today within a distributed security team is a challenge – as highlighted by 51% of organizations.

Risk of data and service unavailability in distributed environments

As organizations move many of their applications and data to distributed, cloud environments, they are increasingly concerned about denial-of-service threats. 39% of organizations are concerned that such threats could prevent legitimate users from accessing their data and applications.

Data and privacy risks due to unsecured application

As application development, deployment and use grows, application security threats are coming to the fore. For 59% of the organizations surveyed, application security still remains an afterthought. Lack of appropriate security controls in applications can often lead to data breach and privacy compromises, thereby putting organizations at financial risk.

Third-party access risks

As organizations strive to improve distribution channel efficiency, supply chains agility and ecosystem collaboration, various stakeholders of the ecosystem are rapidly being integrated through digital platforms. However, providing access to partners, customers, contractors and others, exposes applications and data of the organizations to myriad external threats. 47% of organizations surveyed this year are concerned about the security risks emanating from such third-party access.

Risk of regulatory complexity and non-compliance

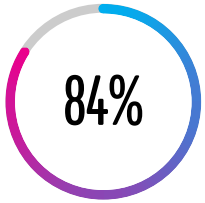
Data sovereignty and privacy regulations at both country and industry levels are evolving to catch up with rapid digitalization and increased cloud adoption. For example, the Dubai International Financial Center (DIFC) Data Protection Law which came out this year, has made significant changes to the existing data privacy law.

The complexity of regulations has grown and often a lack of clarity on its components hampers compliance. 40% of organizations surveyed are concerned about ensuring compliance to regulations. Compliance is in itself beneficial to security improvement. On the other hand, non-compliance is a significant risk that could also lead to penalties and erosion of customer trust.

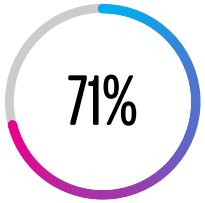
KEY FOCUS AREAS FOR SECURITY INITIATIVES

IN order to address the risk priorities described above, and to build security capabilities, organizations in the Gulf are planning to invest in the following key areas. As they implement initiatives in these areas, they need to consider key recommendations mentioned below to ensure success.

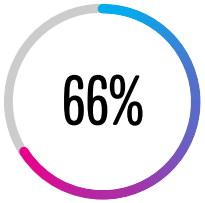
KEY SECURITY AREAS OF FOCUS IN THE NEXT 6 - 12 MONTHS



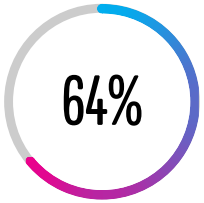
Data Security



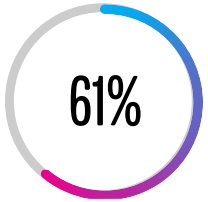
Secure remote access and Connectivity



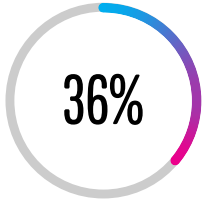
Cloud Security



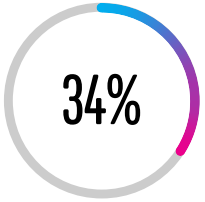
Identity & Access Management



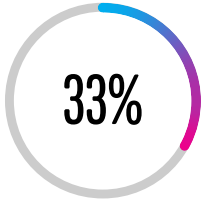
Endpoint Device Management



Secure Application delivery



Security Responce Automation



Virtual Workspaces

Source: GBM Survey October 2020; UAE, Kuwait, Oman & Bahrain; N=70

DATA SECURITY

84% of organizations surveyed are planning to invest in data security over the next 6 to 12 months. Securing data is foundational to building trust with customers today. Data and privacy frameworks that protecting organizations from financial liabilities are also becoming critical.

With the imminent availability of 5G, cloudadoption acceleration, and application explosion, data growth will further accelerate. To extract value from growing volumes of high variety data, organizations will need to develop robust data strategies.

Data discovery and classification are the initial steps organizations need to take on the data security journey. Yet this is a major challenge and weakness for almost 1 out of every 2 organizations surveyed.

As data becomes increasingly distributed, and more sophisticated data regulations are launched by various regulatory authorities - such as the Personal Data Protection Law (PDPL) in Bahrain, DIFC Data Protection Law etc. - managing data security and compliance is becoming increasingly complex. Securing data needs critical thinking from the ground-up involving the mapping of the entire journey of data whether in transit, in use or at rest, and designing visibility and protection mechanisms at all points.

Essential Guidance

DEVELOP A HOLISTIC APPROACH TO DATA PROTECTION

Businesses understand they must be prepared for data loss scenarios, and therefore, are developing disaster recovery plans. However, loss prevention and recovery do not equate to protection. What is missing in many organizations is a holistic and all-encompassing approach to data protection. It is essential for organizations to have a clear understanding of what comprehensive data protection entails, and then to be able to define a roadmap, move along it stage by stage (Data discovery -> data classification -> data leakage prevention), and eventually close the maturity gap.

IMPLEMENT DATA ENCRYPTION AND KEY MANAGEMENT

As data and privacy frameworks evolve and mature, securing data with encryption should become a priority. Organizations must consider careful implementation of encryption mechanisms. Encryption can vary from obfuscation to tokenization to masking, and each has its own use case and trade-offs. Furthermore, as organizations continue adopting cloud, key management must be carefully moderated and models such as bring your own key (BYOK) should be adopted using hardware security modules (HSMs).

INTENSIFY FOCUS ON REGULATORY COMPLIANCE

56% of organizations in the Gulf are adopting frameworks to comply with local and international regulations. Compliance with regulations is extremely useful for designing security from scratch. Not only does it help in ensuring adherence but also to assess the maturity level of the organization. Enhancing compliance with broader implementation of advanced frameworks (such as NIST CSF, CIS CSC, or CSA CCM for cloud) is beneficial.

IDENTITY AND ACCESS MANAGEMENT

64% of the Gulf organizations surveyed say that identity and access management is a key security focus area for the coming 6 to 12 months.

Securing access to critical business applications, services and data is critical for digital enterprises to succeed. Identity and access governance and lifecycle management are at the center of securing the digital enterprise. 57% of organizations surveyed in the Gulf say that their top challenge today is ensuring secured access to digital services for their customers.

Managing the identity lifecycle of users is more critical now than ever before as the workforce is now more distributed, and organizations are striving to augment employee and partner experiences as they move forward into 2021 and beyond. As we move towards a password-less future, access will have to be determined by context - from where you are logging in, at what time and from which device. As organizations leverage mobile applications for direct interfacing with customers, technologies such as customer identity and access management (CIAM) will increasingly come into mainstream usage.

Furthermore, methodologies such as Zero Trust are forcing organizations to rethink least-privilege approaches to access. With organizations adopting cloud, IoT, and mobile platforms, the domain is no longer defined by a fixed location, and therefore, organizations will eventually want to ensure that least-privilege is the de-facto state.

Many organizations are moving towards a hybrid, multi-cloud environment. Building security controls for this environment is difficult - 66% of organizations surveyed say that rolling out the access rules and controls for various cloud environments is a key challenge. As attacks become more sophisticated and privileged accounts continue to be the top targets for adversaries, organizations will need to constantly monitor internal and external privileged users and ensure that anomalies are identified and responded to in a timely manner and in tight integration with security operations. This can be achieved by implementation of privileged access management solutions.

Essential Guidance

IMPLEMENT AN IDENTITY LIFECYCLE MANAGEMENT PROGRAM (ILMP)

An identity lifecycle management program is essential for organizations aiming to achieve control of end-user access rights. The Identity Lifecycle Management program must include the right mix of technologies and processes. Organizations must also have a governance plan in place for periodic assessment of access roles and rights as part of the ILMP. At its core, organizations should implement the following elements to strengthen the program.

- Identify business applications, roles and user access levels that should be part of the ILMP. This helps to define the rule sets that should be rolled out to the identity and access management (IAM) solution. Identification of business rule sets is currently a challenge for 47% of organizations surveyed.
- An optimized ILMP helps organizations to not only securely manage the lifecycle of the user but also to derive direct return on investment (ROI). ROI is achieved by considerably reducing the time the helpdesk team takes to create and manage identities. Today, 27% of Gulf organizations face reluctance from business owners when implementing ILMP. Hence, security leaders must take an ROI-based approach to onboard the business stakeholders in this critical project.
- Take a phased approach to technology adoption in you ILMP: This begins with implementing Identity and Access Management solutions (IAM), with Single Sign On (SSO) and Multi Factor Authentication (MFA). Once these solutions are appropriately implemented and optimized, organizations must improve the maturity of their ILMP with advanced technologies such as Privileged Access Management (PAM) to protect, monitor and audit administrator activities, and User Behavior Analytics (UBA) to detect insider threats and attacks.

CLOUD SECURITY

Securing cloud is a significant focus area for 66% of the surveyed organizations for the next 6 to 12 months. As cloud adoption accelerates and complex data flows are rapidly created to deliver digital use cases, cloud security will become critical to protecting data and applications.

86% of the surveyed organizations say that ensuring their cloud usage is in compliance with local laws and data sovereignty regulations is imperative . Furthermore, as they rapidly move towards a hybrid multi-cloud environment, authentication is becoming more important – 92% of the surveyed organizations say that having strong authentication mechanisms is important for securing their cloud environment.

Robust service level agreements (SLAs) are also key to enabling and governing cloud – 80% of surveyed organizations cite this as an important factor that affects cloud security.

Organizations must understand and document the responsibilities of both parties in the agreements. For instance, in a public cloud the responsibility for security is shared between the Cloud Service Provider (CSP) and the customer organization. The CSP owns the security of the physical layer and the infrastructure of the cloud while the customer is responsible for the security of operating systems platforms, data and applications. Having strong security configurations in IaaS or PaaS models is cited by 68% of Gulf organizations as important to ensuring continuous security of services provided by the CSP.

Essential Guidance

SIMPLIFY CLOUD SECURITY

Cloud security can be simplified to a great extent by implementing the following controls

- Cloud Security Posture Management: Misconfigurations in the cloud environment can lead to serious security issues. To counter misconfigurations and data breaches, organizations should consider adoption of Cloud Security Posture Management (CSPM) tools. A CSPM tool will help to continuously monitor the enterprise cloud environment to identify gaps between policy and actual posture.
- Finer controls with CASB: A Cloud Access Security Broker (CASB) is a security policy enforcement point that exists between the cloud customer and the CSP. A CASB solution can be immensely helpful in governing an organization›s cloud usage with granular visibility and controls. This helps organizations in securing data and improving protection against threats.

GENERAL CONTROLS

Organizations should create baseline controls when adopting cloud. These controls can range from SLAs, authentication mechanisms, data sovereignty and visibility mechanisms to ensure privacy and data security in the cloud environment. Organizations can consider adopting cloud security frameworks such as Cloud Security Alliance Cloud Controls Matrix (CSA CCM) and creating a Unified Control Framework (UCF). A UCF can be created by collating relevant controls from different security frameworks which can be tracked in a consolidated manner.

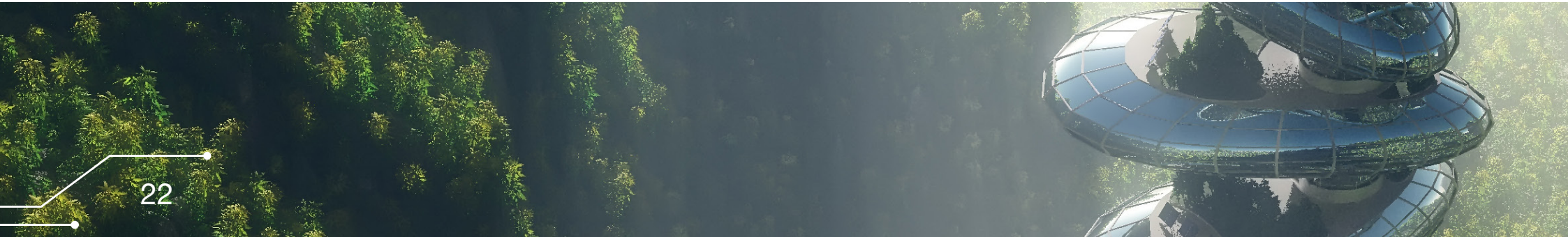
AUTOMATION OF THREAT MANAGEMENT AND SECURITY RESPONSE

Automating security response is a key focus area for 34% of the surveyed organizations for the next 6 to 12 months. Continuous threat monitoring and response assist in mitigating unavailability of critical business services and applications along with providing the benefits of data and privacy vigilance.

Like in many other parts of the world, the volume and sophistication of threats in the Gulf is on the rise. The threats vary from end-user phishing attacks, identity breaches, and ransomware attacks to more sophisticated advanced persistent threats (APTs).

To strengthen threat management and response, 33% of Gulf organizations are reassessing the maturity of their security operations. A few of them are building modern SOCs with cloud-native analytics that combine Artificial Intelligence (AI) and Machine Learning (ML) and User and Entity Behavior Analytics (UEBA). This will enable them to monitor their entire infrastructure landscape, including endpoints, network, and cloud. This will also further help in developing proactive protection, detection and response capabilities, under the overarching theme of security frameworks such as Zero Trust.

Automation in security brings together multiple benefits apart from the obvious benefit of reducing false positives and faster filtering of threats. Organizations can also achieve resource optimization and bridging of security skill gaps – 64% of Gulf organizations currently face challenges in addressing skill gaps. Furthermore, many leading organizations in the Gulf are considering implementation of SOAR (Security Orchestration, Automation, and Response) platforms to automate, orchestrate and measure security operations and incident response processes and tasks, all from within a single, integrated platform. Automation initiatives must be complemented by Cyber Range Simulations and runbooks that help to predict attack vectors and be prepared for them. Threat management and runbooks development is currently a challenge for 57% of Gulf organizations, however, these challenges will decrease in severity as organizations mature and adopt complex use cases in security.



Essential Guidance

ADOPT ADVANCED SECURITY SOLUTIONS

Organizations building their own SOCs must develop a strategy covering technology, people and processes. The technology stack must include advanced security solutions such as Security Orchestration Automation and Response (SOAR), Cross Layered Detection and Response (XDR), Network Detection and Response (NDR) etc. Technologies must be complemented by exhaustive runbooks and a team of capable security analysts.

AIM FOR NEAR-REAL TIME THREAT DETECTION AND RESPONSE

As the skill gap widens and organizations find it challenging to keep scaling up with the security technology stack, they need to consider adopting managed security services (MSS) to address complex use cases. Managed security services from a provider can enable faster threat detection and response which can help to reduce the overall impact of an incident. Furthermore, while procuring services from an MSS provider, it is important that customers perform independent and periodic maturity assessments of the MSS provider.

APPLICATION LIFECYCLE SECURITY

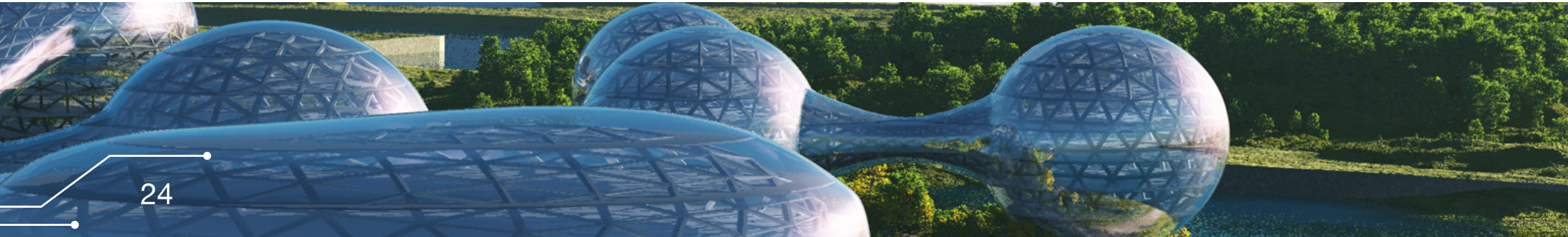
Securing the application lifecycle is an important focus area for 36% of Gulf organizations.

While 41% of organizations surveyed realize the importance of security in software development, 59% feel that application security is still an afterthought in their organizations. Security must be factored into all stages of the lifecycle - design, development, testing, deployment and maintenance.

DevSecOps has brought about a culture shift in software development. These practices were able to “bake” security into the rapid-release cycles that are a typical part of modern application development and deployment (this is often referred to as the DevOps Movement or «Shift left»). The shift to DevSecOps was intended to embed security testing into the Continuous Integration (CI) and Continuous Delivery (CD) pipelines and to build the knowledge and skills needed within the development team so that testing and security bug-fixing can also be done internally.

Though DevSecOps brings its own set of advantages, it works best when implemented in organizations that undertake large scale development activities. However, not many organizations in the Gulf undertake development themselves; most prefer to outsource development to external providers. After development, these custom-built applications are hosted in on-premise environments or on public clouds. Many organizations are also now moving towards container and docker-based environments wherein container-based security is becoming a key priority.

Organizations that have implemented DevSecOps, must now look beyond it to secure their applications further. Organizations should consider implementing controls available in existing local frameworks or globally available frameworks such as NIST Cyber Security Framework CSF, ISO 27001, STRIDE (for threat modeling), or ISO 27034 (an application security framework) to identify controls. However, extending these security controls and implementing them across the application environment is a significant challenge for about 50% of Gulf organizations.



Essential Guidance

FOCUS ON SECURITY ASSESSMENT

When designing an application, attention should be given to controls for application protection. Practices such as source code assessment, common configuration issue assessment, and periodic pre- and post-production technical assessments should be implemented. 69% of Gulf organizations say they plan to conduct thorough technical security assessments at multiple stages of development, deployment and production. It is imperative that organizations adopt Application Security Testing Solutions (DAST / SAST - Dynamic / Static Application Security Testing and open source code security) within the application development and deployment process. Such a phased security assessment approach helps ensure security at multiple stages of the application development to deployment cycle.

DEPLOY WEB APPLICATION FIREWALLS (WAF)

Technical solutions such as web application firewalls also play a key role in continuous protection of applications and therefore, should be integrated into the DevOps environment. A WAF helps protect web applications by filtering and monitoring the HTTP traffic between the application and the Internet. Being a protocol Layer 7 defense (in the OSI model), it provides protection from typical web application attacks such as cross-site scripting (XSS), SQL Injections, and session hijacks, among other OWASP Top 10 web application security risks.

SECURE CONTAINERS

Container security is the process of implementing security tools and policies to protect the infrastructure, software supply chain and runtime. It is essential that security and infrastructure teams enact proper access control measures to protect containers. A least-privileged access model, where container activity is explicitly whitelisted can ensure that users only perform commands based on appropriate controls. As organizations move their critical workloads to cloud, securing containers is critical for runtime security.

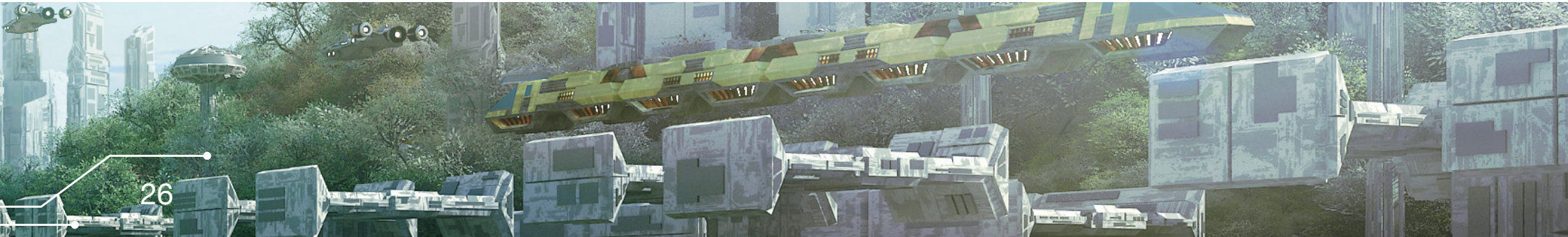
A PARADIGM SHIFT IN NETWORK

Securing access and connectivity for a distributed workforce is a key focus area for 71% of Gulf organizations. As organizations witness a shift from "connect -> authenticate" to "authenticate -> connect", securing access and connectivity becomes critical.

Roughly 80% of network traffic in a datacenter usually flows betweenthe internal systems - this is usually referred to as «East-West» traffic. This traffic is generally not inspected by a firewall. However, a significant risk could arise if an attacker gets through or bypasses perimeter security. Lateral movement to other systems from a compromised system and subsequent navigation within the environment could become much easier for the attacker.

Due to the expansion of the distributed work environment this year, 56% of Gulf organizations are facing an increase in the number of attacks on their infrastructure. At the same time, the number of users connecting from outside the internal network has increased rapidly. This combination of increasing threats and users has made the security control of devices challenging - 57% of surveyed organizations has cited this as a challenge.

Organizations that are reimagining security for the future digital enterprise are re-designing defense-in-depth by following mature security frameworks such as the Zero Trust Network Architecture and distributed integrity models. Zero Trust model in a distributed environment is a proven methodology for reducing the attack surface and improving security at the same time. The adoption of (Micro–segmentation) is also necessary as it can deliver visibility and control of network activity from, and to, every asset. Micro-segmentation involves creating controlled isolated workloads within a datacenter or cloud which enables the network to provide more granular security.



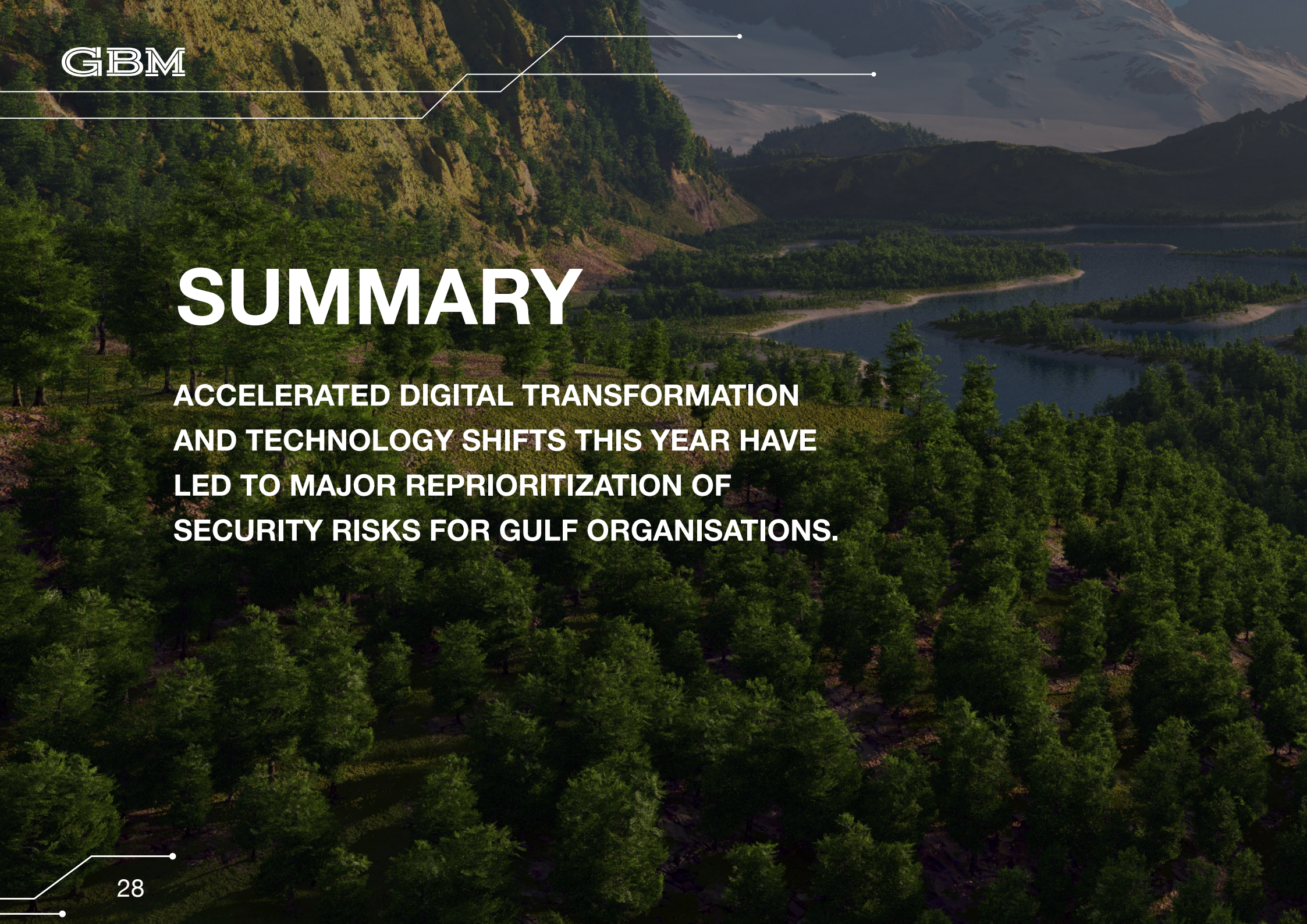
Essential Guidance

EMBRACE NEW MODELS FOR PERIMETER-LESS ARCHITECTURE

Network security has come a long way in the last decade. As cloud becomes a core platform for organizations, it is essential that they embrace new models when designing an identity-driven network architecture. The 2 essential models to consider are

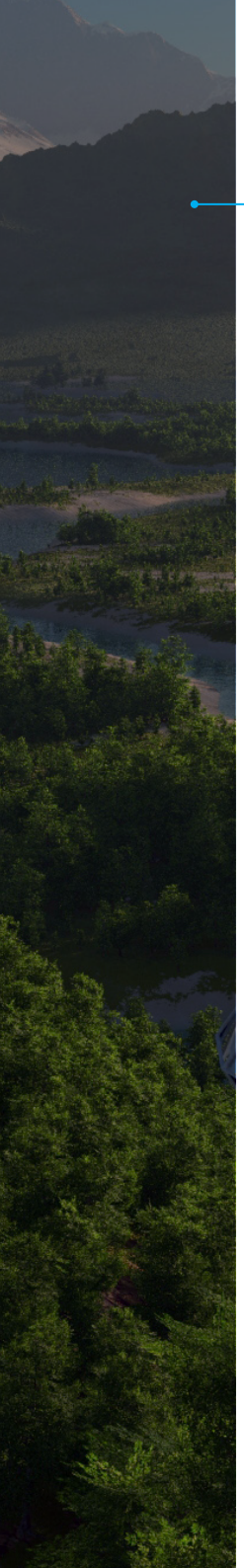
- **Zero Trust Network Architecture (ZTNA):** The Zero Trust framework operates on an adaptive trust model, where trust is never implicit, and access is granted on a «need-to-know», least-privileged basis governed by granular policies. ZTNA helps improve agility and scalability, enabling digital ecosystems to work without exposing services to unauthorized users. This approach helps reduce various risks and threats.

- **Secure Access Service Edge (SASE) model:** With an expansion of the distributed workforce and an increase in the use of SaaS applications, more traffic is moving between the datacenter, the cloud and the branch offices. SASE is the convergence of wide area networking (WAN), and network security services like CASB, DLP, VPN, Secure Web Gateway (SWG), Web Proxy, Firewall)/ Next Generation Firewall (NGFW) and Zero Trust etc. into a single cloud-delivered service model. The SASE model helps not only to reduce costs and consolidate security controls for the organization but also to increase performance and flexibility.



SUMMARY

ACCELERATED DIGITAL TRANSFORMATION AND TECHNOLOGY SHIFTS THIS YEAR HAVE LED TO MAJOR REPRIORITIZATION OF SECURITY RISKS FOR GULF ORGANISATIONS.



As customer needs and preferences shift in the region, organizations across various sectors including government, banking and financial services, healthcare, education, retail and others, are increasingly expanding their portfolio of digitally-augmented products, services and experiences. The workforce has become more distributed this year than ever before with organizations focusing on enabling employees to work from anywhere and providing secure remote access to applications and data

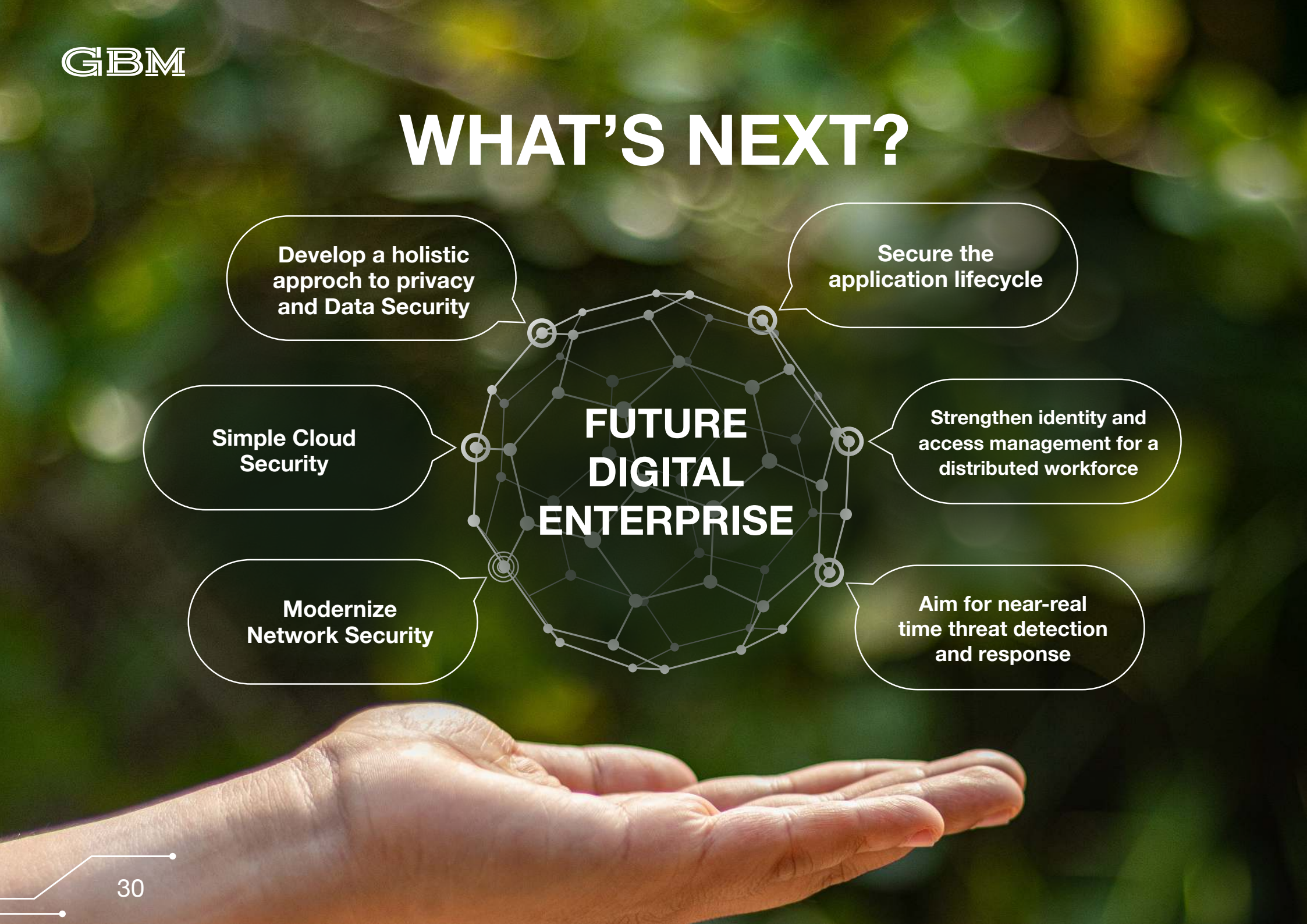
This year is also being shaped by 3 technology shifts in the Gulf – 1) an acceleration in cloud adoption to enable digital initiatives and rationalize IT costs, with organizations increasingly moving towards hybrid, multi-cloud environments 2) an unprecedented shift towards a distributed work model fueling a rapid shift towards tech-enabled collaboration 3) an explosion in the development and deployment of applications across mobile, cloud and on-premise environments, to enable new digital use cases and to support the distributed workforce.

These technology shifts have led to a reprioritization of risks this year from 2019. End user security risks, the risk of cloud security breaches, identity risks, and data and privacy risks have come to the fore. Additionally, the risk of internal delays to incident response, the risk of regulatory complexity and non-compliance, data and service unavailability risks, and others, have become more important than earlier.

To address these risks, organizations in the Gulf are prioritizing their initiatives around a few key focus areas: data security, cloud security, identity and access management, application lifecycle security, automation of threat management and security response, and modernizing network security.

GBM

WHAT'S NEXT?



Develop a holistic approch to privacy and Data Security

Data security and privacy have become key considerations to comply with local and international laws even as the cost of data breach increases. Organizations should create clear data security goals and initiate data mapping exercises to classify data and govern data optimally. These efforts must be complemented by technology that protects data throughout its lifecycle.

Simplify Cloud Security

Organizations will continue to move their workloads to the cloud environment to reduce cost, enable digital use cases, and boost the productivity of the distributed workforce. Organizations must consider implementing solutions such as CASB and CSPM to enhance security in the cloud. As they increasingly move towards hybrid, multi-cloud environments, they also need to enable strong authentication mechanisms, create rock-solid SLAs with CSPs and manage compliance with data sovereignty regulations.

Modernize Network Security

Network security has come a long way and has undergone a massive shift towards leveraging software for defining a perimeter-less world. Organizations adopting public, private, or hybrid cloud models must consider implementing newer technologies that bring more visibility and control than traditional network architecture models. Organizations should consider technologies and models such as Micro-Segmentation, SASE and ZTNA models to modernize network security to support digital transformation initiatives.

Secure the application lifecycle

The heavy dependence of digital transformation on applications is pushing organizations to focus on application security from development to deployment. Organizations must ensure that application security assessments are conducted at each critical phase. Leveraging technologies such as SAST/DAST, Open Source Security, WAF and container security is important while deploying applications in a cloud environment.

Strengthen identity and access management for a distributed workforce

The workforce today is becoming increasingly digitally-savvy and distributed across locations, 64% of Gulf organizations plan to transform existing identity management solutions by orientating it towards role-based access. These solutions and corresponding security controls must be extended not only to the distributed workforce but also to the administrators, power users, and 3rd party users of the enterprise.

Aim for near-real time threat detection and response

The rapidly expanding digital footprint of organizations coupled with the continuously growing threat landscape presents significant challenges to threat management capabilities. Add to that a growing skill gap and the constant difficulty in keeping up with evolving security technologies. Gulf organizations must consider incorporating greater automation into their threat management programs to tackle these challenges. Technologies such as SOAR complemented by incident response planning and cyber range simulations can help organizations further improve their threat management capabilities.

GBM

Author

Hani Nofal
VP of Digital Infrastructure Solutions
Hani@gbmme.com

For questions please contact:

Irmak Parlat Yilmaz
Alliance Marketing Manager
Irmak@gbmme.com +971 4 316 2373

About GBM

With more than 30 years of experience, 7 offices and over 1500 employees across the region - Gulf Business Machines (GBM) is an end-to-end digital solutions provider, offering a broad portfolio, including digital infrastructure, digital business solutions, security and services.

GBM has nurtured deep partnerships with some of the world's leading technology companies and have invested in skills and resources to assist their customers on their path towards digital transformation. As IT continues to be a major driver and enabler of business across the region, its increasing influence is changing the way people live, work, collaborate and make decisions; this requires smarter IT solutions that GBM is uniquely placed to provide.

GBM understands the various challenges faced by CISOs and has built a robust cybersecurity framework, comprised of solutions and services, to protect organizations with IT security industry best practices and enhanced risk mitigation. The framework addresses traditional and emerging challenges faced by organizations and leverages best-of-breed solutions from partners with proven security expertise. GBM offers solutions and services in the following areas to mitigate the increasing risks facing businesses today.

- GBM focuses on people, processes and technology to provide a holistic approach to mitigating risk.
- The GBM framework effectively safeguards brand name, reputation and assets.
- GBM offers comprehensive, end-to-end strategies that protect against external and internal threats and which may include solutions for endpoint security, applications, database, people and regulatory compliance.


GBM
www.gbmme.com