MIDDLE EAST CYBERSECURITY ODYSSEY

EXPLORING THE MIDDLE EAST CYBERSECURITY MARKET POTENTIAL

BROUGHT TO YOU BY

معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC GLOBAL

FROST & SULLIVAN

Evolving Digital Ecosystem in the Middle East

The Middle East has been experiencing rapid digital transformation over the past few years, and this trend is expected to continue in the coming years. Countries in the region are striving to reduce their dependence on oil exports and boost economic growth by investing in emerging technologies like artificial intelligence (AI), cybersecurity, digital infrastructure, renewable energy, and smart cities. Over the past few years, the region has made remarkable strides in its digital transformation journey and is well on its way toward achieving a fully digitized economy and smart cities. Governments have launched various initiatives to support the growth of the digital economy and attract investments.

In April 2022, the UAE government launched the "UAE Digital Economy Strategy" to increase the digital economy's contribution to the non-oil GDP by 20% (by 2031).

UAE and Saudi Arabia have launched several initiatives such as "UAE AI Strategy 2031," "Digital Dubai," and "Vision 2030" to develop AI-based solutions and diversify their economies, including plans for an AI university, research park, paperless strategies, digital health, and building a smart city called "NEOM".

The Middle East has undergone a digital revolution, increasing its dependence on digital tools and technologies. This has made businesses more vulnerable to cyber threats. Geopolitical instability worldwide has heightened the challenge, necessitating stronger cyber defences. The region's digital transformation has shifted its economy, prompting businesses to prioritize cybersecurity. Governments and enterprises have responded by swiftly developing adaptable cybersecurity strategies.

According to Frost & Sullivan, the GCC cybersecurity market is expected to grow threefold by 2030.

$4.8
BILLION
2022

$13.4
BILLION
2030

Saudi Arabia boasts the largest share in the region, with over 60% of the market, followed by the UAE.

Both countries are at the forefront, leading the way in terms of their cybersecurity regulations, technological advancements, workforce development, and strengthened cyber strategies.

The GCC will continue to witness an acceleration of digital transformation initiatives. It is imperative for the governments and enterprises in GCC to protect their digital assets, as implementing cybersecurity solutions is no longer a choice but a critical component for success.

Middle East Braces for Escalating Cyber Threats as Region is Highly Prone to Cyber-Attack

Over the past few years, the region has been a victim of cyberattacks by multiple ransomware groups such as LockBit, Conti, AvosLocker, and Snatch, as well as advanced persistent threats (APTs). These attacks have mostly targeted critical sectors such as oil & gas, manufacturing, information technology (IT)/information technology-enabled services (ITeS), construction, and healthcare. The Middle East is highly vulnerable to several cyberattacks—distributed denial-of-service (DDoS), phishing, malware, SQL injection, man in the middle, DNS tunnelling, and more.

In March 2023

Ransomware incidents in the UAE saw a substantial reduction of over 70%

at the beginning of 2023 compared to the same period in 2022.

UAE successfully prevented over

71 million ***attempted cyber-attacks***

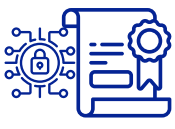
during Q1, Q2, and Q3 of 2023.

Additionally, the country was actively repelling more than

50,000 ***cyber-attacks*** ***on a daily basis in 2023, as stated by UAE Cybersecurity Council***

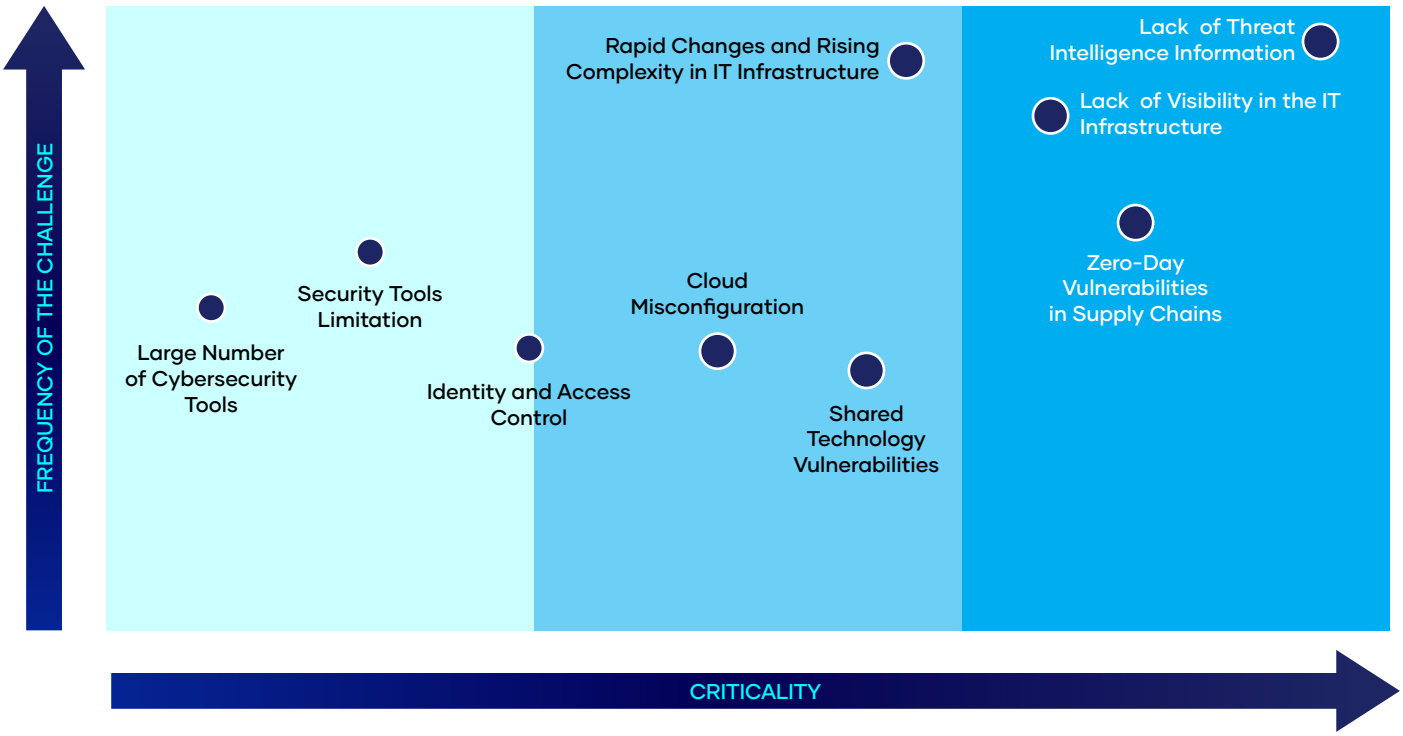
In the Middle East, cybersecurity awareness is pivotal amid rapid digitization and a growing threat landscape. Challenges include low employee awareness and a scarcity of skilled professionals. Very few business leaders are confident in handling cyber-attacks proactively.

To address this, initiatives are underway- Industry-led campaigns aim to boost employee awareness, while educational programs offer courses and workshops on cybersecurity.



Universities in the region provide cybersecurity-related courses to train a new generation. Training programs and certifications focus on equipping individuals with practical cybersecurity skills, working to bridge the existing skills gap.

Enterprises Grapple with Developing a Strong Cybersecurity Foundation



In the modern era of digital technology, businesses encounter numerous cybersecurity challenges that require constant vigilance. The ever-changing landscape of cyber threats, which includes advanced phishing tactics and ransomware attacks, continually jeopardizes the security of sensitive data and business operations. Furthermore, as IT infrastructures become more intricate and remote work becomes the new normal, the attack surface has expanded significantly. This underscores the importance of businesses focusing on robust and all-encompassing cybersecurity strategies.

However, GCC Countries Takes Confident Steps Towards Building Cyber Resilient Posture

The Middle East is actively pursuing cyber resilience by implementing several critical measures. Saudi Arabia, UAE, and Bahrain have established the National Cybersecurity Authority (NCA), the National Electronic Security Authority (NESA), and the National Cyber Security Center (NCSC), respectively, to oversee cybersecurity efforts. Additionally, these countries have established CERT and introduced personal data protection laws (PDPL) to protect citizen privacy and govern the flow of data in the country, as well as cross-border transfer of data. These laws also impose heavy penalties for non-compliance—Saudi Arabia's PDPL imposes fines of up to SAR 10 million and imprisonment.

The GCC countries need a robust cybersecurity strategy that includes GRC measures, business continuity, incident response, and disaster recovery planning.

Cybersecurity capacity building, advanced security solutions, and regular awareness training for employees are essential to quickly detect and respond to threats, as the attack surface continues to expand with digitalization.

The proactive measures taken by the Middle East governments—launch of cybersecurity initiatives and establishment of industry bodies—demonstrate commitment to safeguarding digital assets and ensuring a secure environment for citizens.

These efforts have paid off, as evidenced by the ITU Global Cybersecurity Index 2020 rankings, where Saudi Arabia ranked 2nd and UAE ranked 5th out of 194 countries worldwide. This underlines the Middle East's dedication to staying ahead of cyber threats and creating a resilient digital ecosystem.

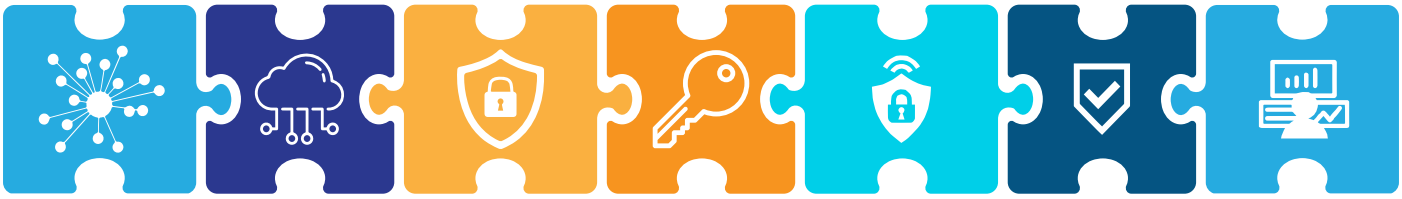
The Fading Legacy Network Perimeter:

Demands Borderless and Boundless Cybersecurity Solutions, Critical for Providers to Offer Solutions Around Cloud Security, Identity Verification, Access Management, and OT Security

Secure cloud journey
Cloud with security by design

Zero Trust
Mindset shift to never trust, always verify

Cyber Insurance
Compensating fincial loss



XDR
Extended Detection and Response

SASE
Cloud delivered networking + cyber security

OT Security
IT/OT convergence

Modern SoC
Enhanced MDR capabilities

According to Frost & Sullivan, there are several strategic areas of focus that both end users and cybersecurity OEMs should pay attention to. These strategic areas are crucial for enhancing cybersecurity preparedness and staying ahead of emerging threats, as Cybersecurity is rapidly evolving with several key trends shaping the landscape.

Secure cloud journeys are becoming paramount, integrating cloud infrastructure with robust security measures. The concept of XDR is gaining traction, offering a comprehensive approach to threat detection and mitigation.

Zero Trust is a mindset shift, emphasizing continuous verification over blind trust. Additionally, the convergence of IT and OT security, along with the rise of cyber insurance compensating for financial losses, highlight the need for a holistic approach to safeguarding digital assets. Modern SoC plays a crucial role in monitoring and responding to emerging threats, ensuring the ongoing security of an organization's digital ecosystem.

By concentrating efforts on these key areas, organizations can fortify their cybersecurity defences and effectively combat the ever-evolving landscape of cyber threats.

Navigating The Digital Landscape:

Compliance and Regulation Remains the Strongest Advocate for Cybersecurity Growth

- Enterprises need to adhere to local regulations such as ECC, CRF, etc., along with industry mandates like PDPL, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), etc. This can be achieved by integrating advanced cybersecurity solutions, which subsequently boost the demand.
- The proliferation of IoT devices has increased organizations' exposure to cyber risks.
- Prevent unauthorized data access and security incidents through real-time security updates and patch management.
- Mitigate threats that occur from the expansion of the attack surface due to complex IT infrastructure.
- The surge in e-commerce and digital banking across the Middle East has generated a heightened need for ensuring security. Both enterprises and individuals are actively seeking robust cybersecurity solutions to protect their financial dealings and personal data.

Middle East is Becoming a Promising Growth Region for Cybersecurity Industry:

Offering Several Growth Opportunities

1. **Security Consolidation and Platformization:** Vendors in the Middle East region are increasingly offering comprehensive, integrated security solutions. The security consolidation and platformization streamlines protection, enhances threat detection, and simplifies management, making it a key strategy to enhance their value proposition in response to the evolving threat landscape. This meets the surging demand for comprehensive cybersecurity services, positioning them at the forefront of the industry's expansion.
2. **Cloud Security:** As cloud adoption continues to rise, the demand for robust cloud security solutions is increasing. Cybersecurity players who meet this demand are poised for growth, as they play a crucial role in securing cloud services.
3. **Adoption of Foundational Security Concepts:** Large enterprises in the Middle East are increasingly adopting foundational security concepts like Secure Access Service Edge (SASE), Security service edge (SSE), and Zero Trust. Cybersecurity firms should focus on developing and implementing these new-age concepts to meet the evolving needs of clients.
4. **IT-OT Convergence:** The seamless integration of traditionally isolated IT and OT domains is crucial for safeguarding critical infrastructure and industrial systems against evolving cyber threats. This convergence creates fertile ground for innovative cybersecurity solutions tailored to protect the interconnected landscape of the digital and physical worlds.
5. **IoT Security:** The IoT devices are expanding in the Middle East. This growth is driven by the need to secure IoT devices and data, leading to increased investments in IoT security solutions, partnerships with global cybersecurity firms, and innovation in the region's cybersecurity ecosystem.

6. **Evolving Cybersecurity Regulations:** Cybersecurity regulations in the Middle East are rapidly changing, with a shift towards industry-specific laws, policies, and guidelines. Enterprises are prioritizing compliance and data protection, driving the demand for innovative solutions and services to safeguard digital assets and customer trust. Enterprises strategically harness industry-specific frameworks to effectively navigate the intricate landscape of compliance requirements, ensuring they stay in alignment with regulatory standards.
7. **Cybersecurity Education and Training:** There's a growing need for cybersecurity education and training programs in the Middle East to address the shortage of skilled professionals in the field.
8. **Supply Chain Security:** With the complexity of supply chains, securing them against cyber threats is crucial. Cybersecurity OEMs can provide supply chain security solutions, while MSSPs can offer monitoring services.
9. **Booming E-commerce and Retail Industry:** The Middle East has witnessed significant growth in e-commerce and retail. This sector requires robust cybersecurity to protect customer data, payment information, and supply chain logistics.
10. **Cross-Industry Partnerships:** Collaborations between OEMs, MSSPs, and SIs can help create comprehensive cybersecurity solutions tailored to specific Middle Eastern industries.

The cybersecurity market in the Middle East is poised for rapid growth due to increasing digitalization and evolving cyber threats. To seize this opportunity, regional stakeholders should prioritize collaboration, innovation, and talent development to protect critical infrastructure and establish the Middle East as a global cybersecurity hub.

Notably, the Middle East relies more on major established cybersecurity OEMs, as they lack homegrown solutions. Government initiatives are also driving progress, with subsequent investments in infrastructure and cyber program.