channelpost
MIDDLE EAST AND AFRICA
www.channelpostmea.com
JULY 2026

NEW CHANNEL ECONOMY POWERED BY AI, SKILLS AND OUTCOMES

The channel is shifting from transactional reselling to outcome driven value creation, as partners build AI expertise, deepen consulting capabilities, and adopt new service models to meet rising customer expectations and deliver measurable business impact across hybrid, data centric environments.

CYBER RESILIENCE POWERING THE MIDDLE EAST'S DIGITAL AMBITION

The region's enterprises are strengthening business continuity through prevention first security, identity centric controls, AI driven detection, and continuous validation, ensuring critical services remain available and resilient even as cyber threats intensify across hybrid, multi cloud, and AI powered environments.

Digital transformation in the region is accelerating at a historic pace, reshaping how governments, enterprises, and critical infrastructure operators build and secure their digital futures. AI powered smart cities are taking shape, cloud adoption is expanding, and automation is becoming central to modern operations. This rapid evolution, however, has dramatically widened the attack surface. Cyberattacks are now more sophisticated, more targeted, and more disruptive than ever before. In this climate, cyber resilience has emerged as the defining capability for organisations determined not only to withstand attacks, but to continue operating through them — maintaining essential services without interruption.

Channel Post MEA spoke with twelve leading cybersecurity experts whose organisations are shaping the future of cyber resilience across the region. Their insights reveal a clear truth: resilience is no longer a technical aspiration; it is a

strategic necessity.

Resilience Begins Before the Attack

For Ilyas Mohammed, COO at AmiViz, resilience is fundamentally proactive. "Modern cyber resilience extends far beyond backup and recovery. The objective is to maintain business continuity by preventing cyber incidents from escalating into business outages," he says. AmiViz's ecosystem integrates continuous monitoring, Zero Trust principles, identity protection, endpoint security, and rapid recovery capabilities. These layers work together to contain attacks quickly and maintain access to critical services even while remediation is underway. Mohammed stresses that resilience must be validated continuously. "Organizations should not assume their recovery plans will work; they must continuously test them," he explains, highlighting automated recovery testing, ransomware readiness assessments, and immutable backup verification as essential components of a mature resilience strategy.

Prevention as the First Line of Defence

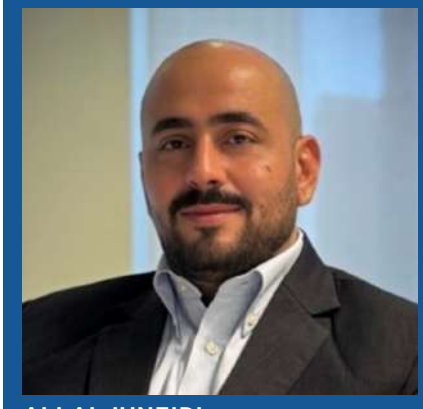
Ram Narayanan, Country Manager at Check Point Software Technologies, Middle East, believes resilience starts with stopping threats before they become incidents. "Cyber resilience begins with preventing disruption before it impacts the business," he says. Check Point's prevention first approach unifies security across networks, cloud, endpoints, email, and SaaS through its Cyber Security Platform. Powered by ThreatCloud AI, the platform correlates global threat intelligence with real time telemetry to identify emerging threats with high confidence. Automated response capabilities isolate affected assets and contain malicious activity across hybrid and multi cloud environments. Narayanan emphasises continuous validation: "Our Agentic Exposure Validation uses AI agents to validate real world attack paths and identify the exposures that matter most."

Visibility: The Foundation of Resilience

For Meriam ElOuazzani, Vice President for Middle East, Turkey, and Africa at Censys, resilience begins with knowing what is exposed. "Recovery assumes you've already lost the fight. Real resilience is architectural," she says. "Segmented networks, redundant failover, traffic that reroutes before anyone notices — but most outages start upstream, with an exposed asset nobody knew was internet facing." Censys provides continuous visibility into internet facing infrastructure, mapping ports, certificates, misconfigured cloud assets, and attacker associated domains. This visibility gives SIEM, SOAR, TIP, and XDR platforms sharper context, enabling faster detection and containment. ElOuazzani notes that resilience validation must be grounded in reality: "The most useful drills are grounded in what's actually exposed on the live internet rather than hypothetical scenarios."

Unified Security for Continuous Operations

Tony Zabaneh, Director, Systems Engineering – South Middle East at Fortinet, defines resilience as the ability to operate securely throughout an attack. "Cyber resilience is about keeping organizations operating securely throughout an attack, not simply recovering once it has occurred," he explains. Fortinet's Security Fabric unifies networking and security under a single platform, enabling integrated visibility, segmentation, and automated policy enforcement. Its unified Security Operations combine SIEM, SOAR, endpoint security, network detection and response, and FortiGuard threat intelligence. "Shared telemetry across the Security Fabric enables real time threat detection, automated investigation, and coordinated response across on premises, hybrid, and multi cloud environments," Zabaneh says. Continuous validation ensures that detection and response workflows remain effective as threats evolve.



ALI ALJUNEIDI
REGIONAL SALES AND BUSINESS DEVELOPMENT MANAGER AT ESET MIDDLE EAST

Lifecycle Protection and Continuous Testing

At Cloud Box Technologies, Vice President Biju Unni emphasises that resilience must span the entire lifecycle of a cyber incident. "Cybersecurity is much more than recovery after an incident," he says. "A series of events unfold before the existing cybersecurity profile crumbles." Cloud Box Technologies delivers continuous monitoring, penetration testing, resilient infrastructure, threat prevention, and automated orchestration. Its 24/7 operations team ensures business continuity across complex IT ecosystems. Unni highlights

BIJU UNNI
VICE PRESIDENT, CLOUD BOX TECHNOLOGIES

HASANIAN ALKASSAB
SECURITY BUSINESS UNIT DIRECTOR, GBM

ILYAS MOHAMMED
COO AT AMIVIZ

MERIAM ELOUAZZANI
VICE PRESIDENT FOR MIDDLE EAST, TURKEY, AND AFRICA, CENSYS

non disruptive recovery testing, VAPT, and ransomware simulation as essential for readiness. "We run RPOs and RTOs to ascertain policy based testing and compliance while identifying gaps that can enable us to improve recovery performance in the future," he explains.

Identity: The Core of Resilience

Mortada Ayad, Vice President – META at Delinea, believes resilience begins with securing identities. "Continuity starts with making sure the credentials that control access to critical systems can't be weaponized or taken offline in the first place," he says. The Delinea Platform enforces least privilege and just in time access across human, machine, and AI identities, ensuring attackers cannot inherit standing privileges to move laterally or disrupt operations. Ayad highlights Resilient Secrets, which replicates a Secret Server instance to a separate, locked down environment every 15 minutes. "Resilient Secrets keeps credentials available when the environment isn't," he explains. "Response teams can retain access to what they need, even if the primary instance is compromised or offline." This identity centric approach ensures that recovery teams always have access to trusted credentials.

Detection and Response at Machine Speed

Ali AlJuneidi, Regional Sales and Business Development Manager at ESET Middle East, reinforces the importance of prevention and early detection. "ESET focuses on prevention, early detection, and rapid response to minimize disruption before incidents escalate," he says. ESET's XDR capabilities combine real time detection, automated investigation, threat correlation, and response actions across endpoints. Security teams can quickly isolate affected devices, contain threats, and maintain centralized visibility across diverse IT environments. AlJuneidi notes that continuous monitoring and proactive threat validation help organisations strengthen resilience without unnecessary operational disruption.

Application Level Resilience

For Zakeer Zubair, Director, Solutions Engineering, Middle East, Türkiye and Africa at F5, resilience is about protecting and managing application traffic before, during, and after an attack. "F5 helps organisations maintain business continuity by protecting and managing application traffic before, during and after an attack," he says. The F5 Application Delivery and Security Platform integrates application delivery, traffic management, API protection, DDoS mitigation, and consistent policy enforcement across hybrid and multi cloud environments. Zubair also highlights F5's Distributed Cloud Web App Scanning, which uncovers exposed apps and APIs, and the F5 AI Red Team, which simulates attacks on AI systems to identify vulnerabilities before adversaries exploit them. "Our AI Security Platform extends visibility, governance, testing and runtime protection across AI applications, models, agents and the APIs connecting them," he explains.

Data First Resilience

Samer Diya, Senior Vice President, EMEA Sales at Forcepoint, takes a data centric view of resilience. "Business resilience starts with reducing disruption before an attack impacts operations," he says. Forcepoint continuously monitors and protects sensitive data across endpoints, cloud, SaaS, and AI applications using adaptive, risk based controls. "Resilience is strongest when the focus is on the data layer itself," Diya explains. Forcepoint's AI Data Security Platform unifies DLP, DSPM, DDR, CASB, web and email security under a single policy framework. This unified approach extends to AI interactions, providing continuous visibility into sensitive data and detecting abnormal activity in real time. Diya notes that recovery testing and ransomware simulation are typically delivered through backup platforms, while Forcepoint complements these investments with continuous data protection and adaptive controls.

MORTADA AYAD
VP OF SALES - META, DELINEA

MUHAMMAD ZUBAIR
CYBERSECURITY PRESALES CONSULTANT AT OMNIX INTERNATIONAL

RAM NARAYANAN
COUNTRY MANAGER, CHECK POINT SOFTWARE TECHNOLOGIES, MIDDLE EAST

SAMER DIYA
SENIOR VICE PRESIDENT, EMEA SALES, FORCEPOINT

SAMER EL KODSI
REGIONAL VICE PRESIDENT, GULF & NORTH AFRICA AT PALO ALTO NETWORKS

Zero Trust and Continuous Testing

At GBM, Security Business Unit Director Hasanian Alkassab defines resilience as the ability to keep the business running during an attack. "Through our GBM Shield framework, we combine zero trust, continuous monitoring, threat detection, network segmentation, and automated response to contain attacks before they disrupt critical operations," he says. GBM Shield delivers defence grade protection and 24/7 unified visibility across hybrid and multi cloud environments.

Its AI powered platform correlates fragmented telemetry in real time, detecting anomalies at machine speed and instantly quarantining affected systems. Alkassab emphasises continuous, non disruptive testing: "We conduct controlled ransomware, DDoS, and recovery simulations to pressure test incident response and business continuity plans." Using isolated recovery environments, GBM validates application recovery, data integrity, and measurable RTO/RPO objectives while ensuring production remains unaffected.

Resilience Across IT and OT

Muhammad Zubair, Cybersecurity Presales Consultant at Omnix International, highlights the importance of protecting both IT and OT environments. "Resilience means being able to operate through an attack, not just recover from one," he says. Omnix builds Zero Trust architectures around privileged access and identity governance, with network segmentation ensuring that a breach in one area does not compromise the entire business.

Self learning AI contains threats within seconds, keeping critical IT and OT operations running even mid incident. Zubair notes that validation must happen before an incident: "We run ransomware simulations, tabletop exercises, and gap assessments aligned with NCA ECC, SAMA CSF, NCA OTCC, and IEC 62443." All testing takes place in isolated replicas of production, allowing clients to refine RTO/RPO targets without impacting live operations.

Platform Driven Resilience

Samer El Kodsi, Regional Vice President, Gulf & North Africa at Palo Alto Networks, believes resilience requires a unified platform approach. "Palo Alto Networks helps organisations maintain operations by preventing attacks, detecting threats in real time, and automating containment before disruption spreads," he says. The company's platformization strategy combines AI driven security, Zero Trust principles, and integrated protection across networks, cloud, endpoints, and identities.

Precision AI powered services strengthen protection across AI ready infrastructure. El Kodsi highlights continuous security validation, attack simulation, ransomware readiness assessments, and attack path analysis as essential for resilience. "Unit 42 also conducts compromise assessments, tabletop exercises and purple team simulations to identify gaps and improve organisational preparedness before a real attack occurs," he explains.

Conclusion: Resilience Is Now the Benchmark of Digital Maturity

Across all twelve perspectives, one theme is unmistakable: cyber resilience is no longer a technical capability — it is a strategic imperative. The Middle East's digital ambitions, from AI powered cities to cloud driven economies, depend on infrastructures that can withstand disruption, adapt to evolving threats, and maintain continuity under pressure.

Resilience today is proactive, data driven, identity centric, and continuously validated. It spans prevention, detection, response, and recovery. It integrates Zero Trust, AI powered analytics, unified platforms, and continuous testing. And most importantly, it ensures that organisations can continue operating even during an attack.

As the region moves deeper into an era defined by AI, automation, and hyper connectivity, cyber resilience will remain the benchmark of digital maturity — the capability that separates organisations that merely survive from those that thrive.

TONY ZABANEH
DIRECTOR, SYSTEMS ENGINEERING, MIDDLE EAST SOUTH AT FORTINET

ZAKEER ZUBAIR
DIRECTOR, SOLUTIONS ENGINEERING, MIDDLE EAST, TÜRKIYE AND AFRICA AT F5