State of the GCC 2025: The Steady Rise of Email Authentication

Despite remaining one of the most exposed vectors in the GCC's digital landscape, email .domains have seen tangible and continued progress year after year

The 2025 edition of the *State of the GCC – Email Authentication* report, jointly published by ORYXLABS and the UAE Cyber Security Council, offers a data-driven view of how domains .across the region are protecting their communications perimeter

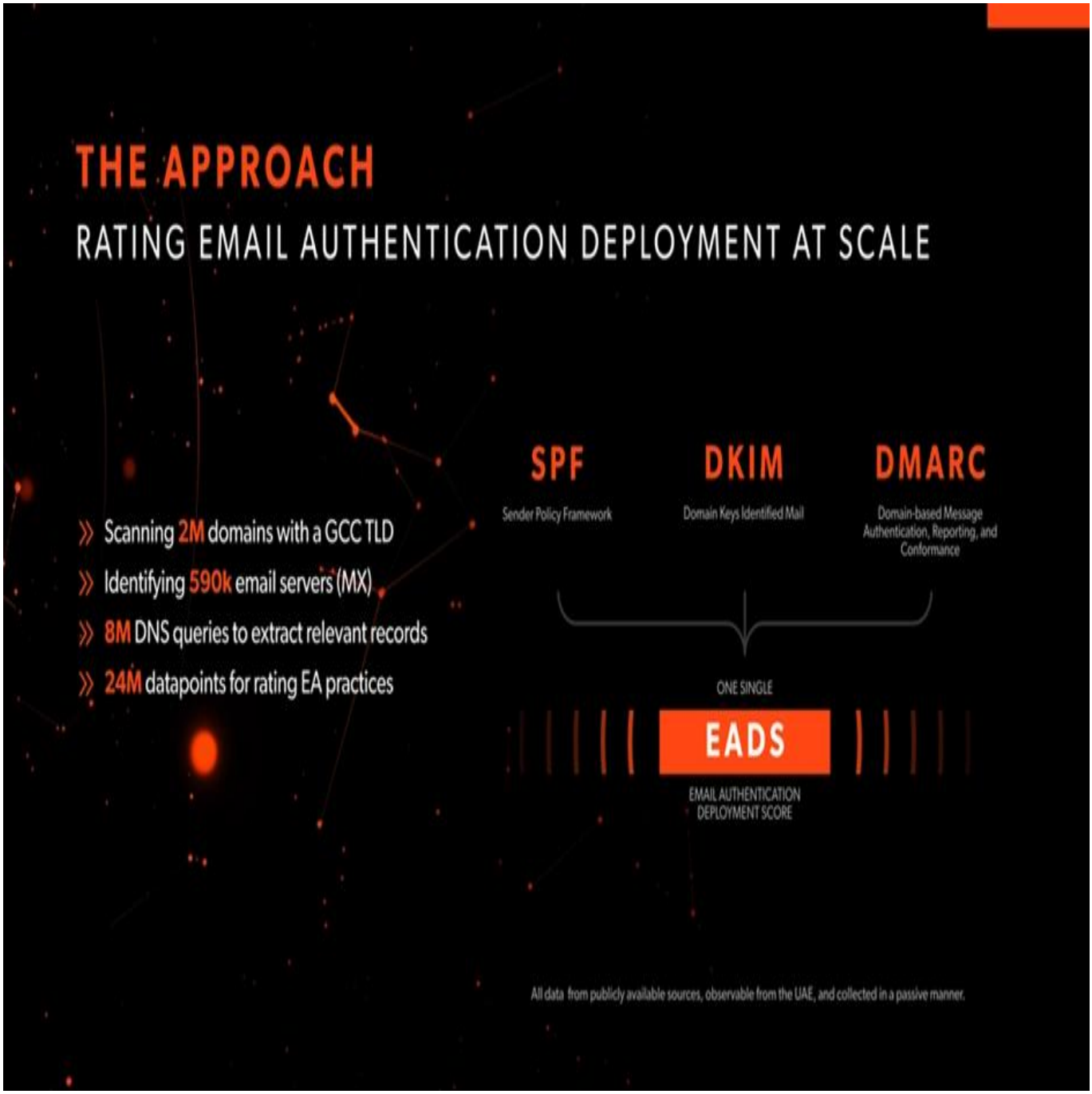
Building on the momentum captured in last year's benchmark report, the 2025 edition .confirms that GCC email ecosystems are maturing – technically, procedurally, and at scale

A Regionwide Assessment

Drawing from more than 2 million top-level domains scanned across the region, the GCC Report identifies and analyses 590,000 active email servers through over 8 million DNS .queries, resulting in 24 million datapoints

The consolidated **Email Authentication Deployment Score (EADS)**, a synthetic metric combining SPF, DKIM, and DMARC adoption and configuration quality, now stands at **32%**, marking a **+3 point improvement** from last year's baseline. This translates to an almost .10% relative increase year-on-year in regional deployment efficiency

Figure: Methodology for EA evaluation

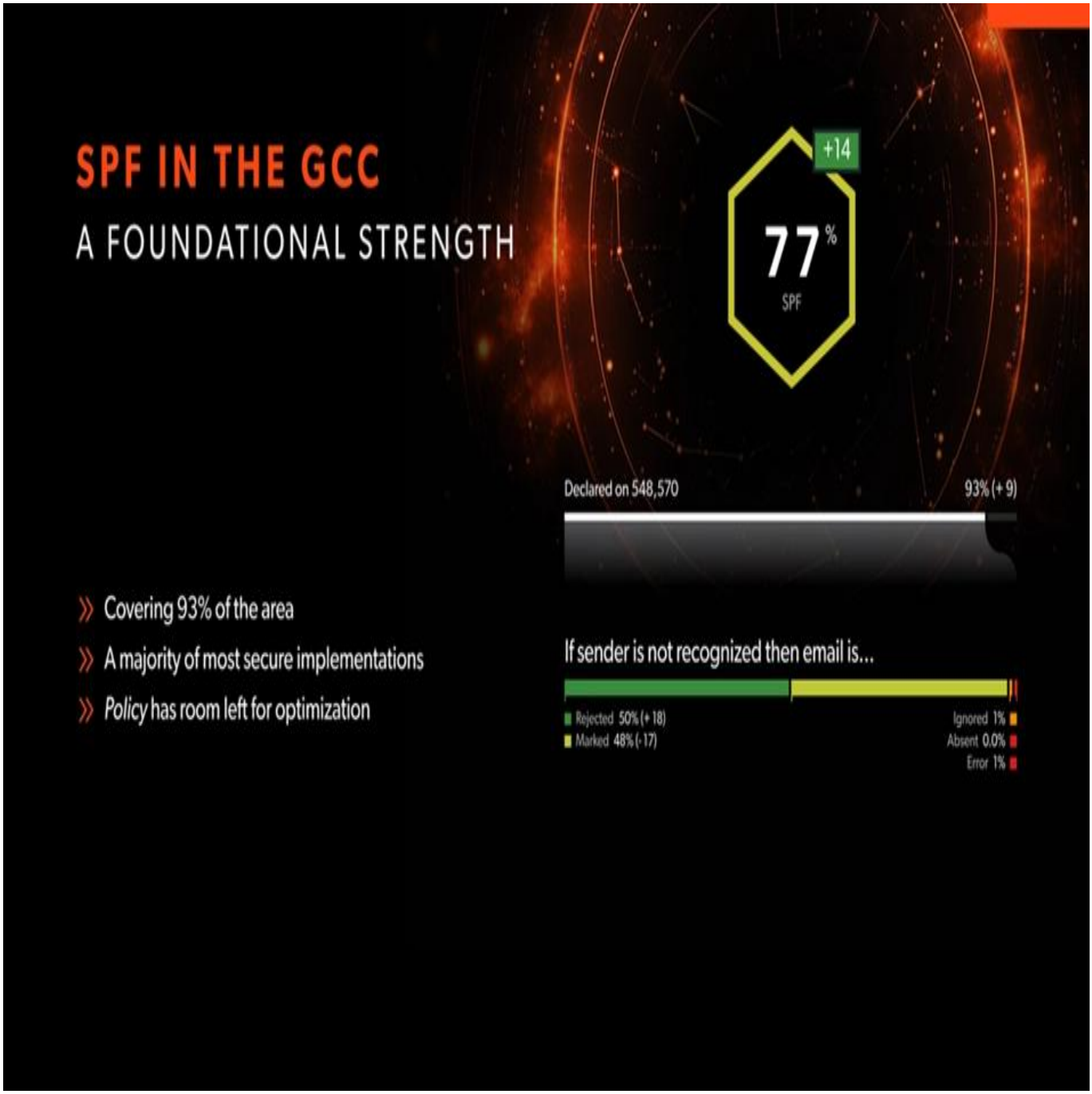


Strong Foundations, Narrowing Gaps

The standout performer this year is **SPF**, reaching **77% efficiency (+14)**. Coverage now extends to **93% of all observed servers**, reflecting how sender verification has become a .near-universal baseline across the region

Half of SPF-enabled domains now reject unrecognised senders outright, up from one-third in 2024 – a significant hardening in policy which reduces exposure to spoofing and business email compromise. This steady migration from permissive to enforcing policies underscores .GCC members' growing operational confidence

.Figure: SPF coverage and policy configuration across GCC domains



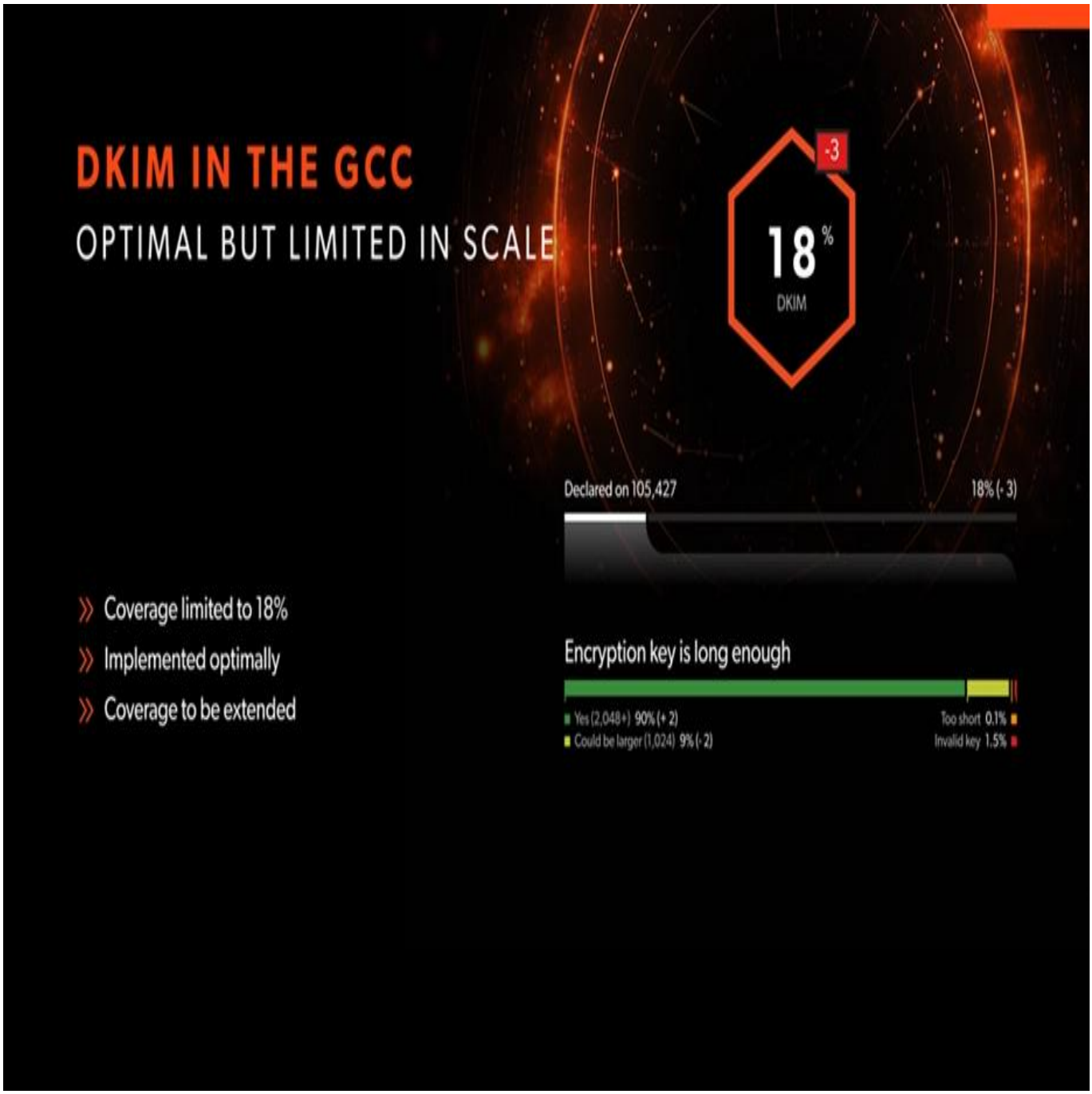
DKIM, by contrast, remains stable in quality but limited in scope. Although **90% of implementations use cryptographic keys of at least 2048 bits**, total coverage .**(**decreased slightly to **18 % (–3**

This limited reach reflects the **operational complexity** of DKIM. Unlike SPF, which depends only on DNS records, DKIM requires precise coordination between mail servers and DNS selectors. In multi-tenant or hybrid environments – common across government and enterprise setups in the GCC – **key management, rotation, and selector synchronisation** often introduce friction. Legacy appliances and fragmented hosting arrangements can further delay deployment. As a result, DKIM tends to be concentrated among **technically mature or centrally managed infrastructures**; broader adoption will depend on the **automation of signing and key-handling processes** across hosted .email ecosystems

This trend suggests that DKIM will mostly feature in particularly well-secured domains,

rather than as a broad regional standard. This may be a future focus area as the GCC .advances in digital maturity

.Figure: DKIM coverage and encryption configuration across GCC domains



Together, SPF and DKIM provide the backbone for authentication in the GCC. However, their combined value still depends on how rigorously DMARC is implemented, in particular where .policy enforcement is concerned

DMARC continues to expand across the GCC, albeit unevenly. Deployment now covers **12% of domains (+3)**, but configuration remains a challenge: only **29%** provide a .reporting address, and **two-thirds still allow unverified messages to pass**

Despite this, enforcement-oriented DMARCs are rising, with 21% of adopters now rejecting failed messages, confirming that enforcement is gradually becoming the standard among .top-tier domains

While SPF signals broad discipline and DKIM marks selective maturity, DMARC remains the .slowest-moving – but one where gradual alignment is visible

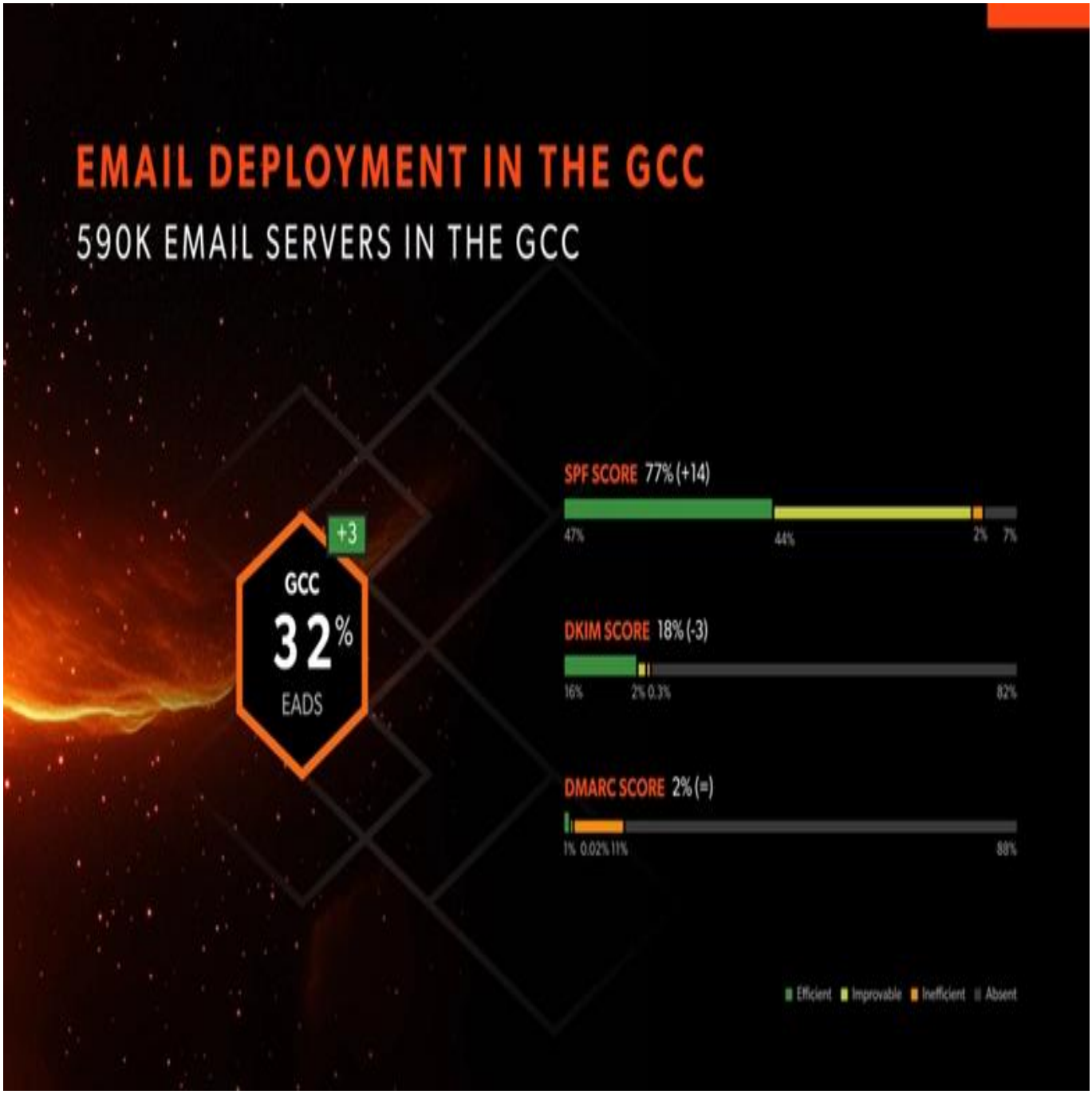
.Figure: DMARC coverage and configuration across GCC domains

Toward Systemic Maturity

The combined picture points to a region in transition: moving from fragmented adoption to .structured governance

SPF's near-ubiquity demonstrates operational discipline, DKIM's selectivity highlights a divide between mature and emerging actors, and DMARC's slow but expanding reach .signals growing awareness of authentication's strategic role in trust and resilience

Figure: Summary of EA protocols configurations across GCC domains



- **Key takeaway:** SPF is now a regional baseline, DKIM an advanced marker, and .DMARC the next frontier for scale and consistency

Email authentication across the GCC is no longer an optional layer; it has become a foundational security protocol, integrated into national and organisational hygiene. The task ahead is to sustain this trajectory through scale, consistency, and accountability, .transforming solid technical gains into systemic resilience

The continued collaboration with the UAE Cyber Security Council ensures this effort remains .regionally grounded and globally aligned

Full coverage and methodology available in the joint publication with the UAE Cyber .Security Council

ORYXLABS

JOINT
PUBLICATION
WITH

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL