

Sophisticated cybercrimes and digital espionage are on the rise due to the financial and economic status of the countries in the Middle East.

Rank **2ND**

According to IBM's Cost of the Security Breach Report 2022, the Middle East is the second-highest region.

Source: IBM



Due to drastic operational shifts, security incidents have become more costly and harder to contain.

Source: ITP

\$7.46M

Average incident cost in MENA Region

Source: SECURITYMIDDLEEAST

Percentage Increase in data breach costs

13% increase since 2021 and 2020

Source: SECURITYMIDDLEEAST

92%



Report increase in attacks versus the prior year

Source: VMWARE

Sectors Most Affected by Data Breaches



Finance



Healthcare



Energy

Source: ARABNEWS

Data Breaches Hurt Reputation



No reputational effect

Negative effect on the reputation

Source: VMWARE

62.5%

Attacks in the financial sector becoming significantly complex

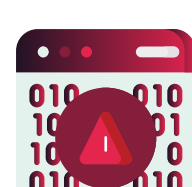
Source: VMWARE



Financial Effect of the Breaches



Source: VMWARE



80%

Changes or increases in the attack landscape affected by COVID-19 require a security rethink

Source: VMWARE

Government Sector – Effect of Breaches



Source: VMWARE



Some negative impact



Severe negative impact



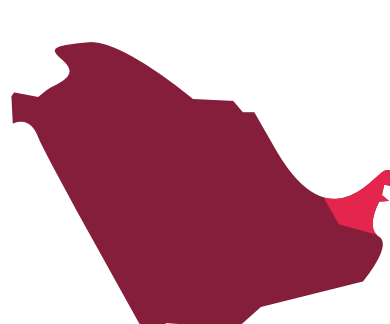
Source: VMWARE

Organizations Hit by Ransomware Attacks

38%

in UAE

Source: CIO



17%

in Saudi Arabia

Cause of Data Breaches

Malicious attacks

59%

System glitches

24%

Human error

17%

Source: SECURITYMIDDLEEASTMAG

Average Time for Companies in KSA and UAE to Detect a Breach



Reduced from

279 days to 269 days



100 days

to contain the breach

Source: SECURITYMIDDLEEASTMAG

Impact of Using Security AI and Automation

Breaches at organizations with fully deployed security AI and automation cost **USD 3.05 million less** than those with no security AI and automation deployed.

Source: IBM



Why

Data-Centric Security in the MENA Region?



Compliance and Privacy regulations like the Saudi Arabian Monetary Authority (SAMA), Saudi Data and AI Authority (SDAIA), UAE Resolution no. 21 of 2013, National Information Assurance Partnership (NIAP), and the Essential Cybersecurity Controls (ECC) & Data Cybersecurity Controls (DCC) of National Cybersecurity Authority (NCA) require organizations to protect critical and sensitive information.

Majority of the Data Privacy Regulations Focus on:



Who can access consumer data?



Consequences of sharing consumer data with vendors



Enforcing strict security policies on the usage and movement of data



Protecting data at the source to eliminate the risks associated with outsourcing, cloud computing, and BYOD

Achieve Data Privacy & Compliance with Seclore Data-Centric Security Platform

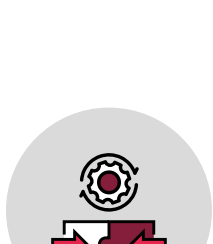
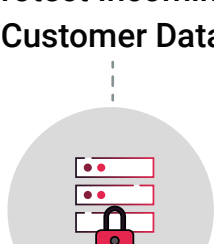
Meet Data Privacy Regulations

Protect Incoming Customer Data

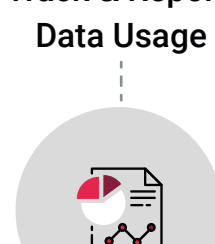
Track & Report Data Usage



Automate Data Protection



Integrate & Automate with Enterprise System



Learn how Seclore helps organizations comply with the NCA regulations.

[Download Whitepaper](#)