

SECLORE'S SECURE 2030: SAFEGUARDING VISION 2030

Vision 2030 Meets Secure 2030

The Future Of Data-Centric Security In KSA

Saudi Arabia's Vision 2030 is driving unprecedented digital transformation, aiming to position the Kingdom as a global leader in technology, innovation, and economic diversification. However, as digitalization accelerates, ensuring data sovereignty, security, and compliance is crucial for sustaining this progress.

Seclore's Secure 2030 initiative aligns with Vision 2030 by providing persistent data-centric security, enabling secure third-party collaboration, and ensuring compliance with national cybersecurity mandates. By protecting critical data assets across industries, Seclore helps organizations embrace innovation while mitigating cybersecurity risks, ensuring that Saudi Arabia's digital ambitions are built on a foundation of trust, resilience, and sovereignty.

This partnership between Vision 2030 and Secure 2030 ensures that Saudi enterprises, government entities, and critical infrastructure can thrive in a digitally connected world while maintaining full control over their sensitive data.



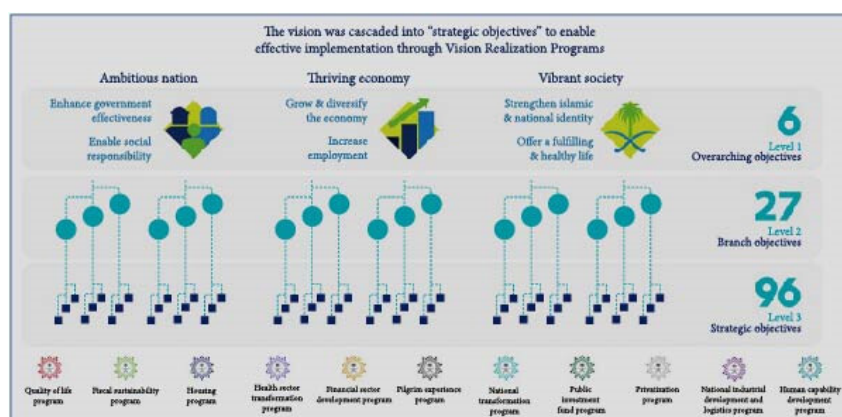
Executive Summary

As Saudi Arabia accelerates its digital transformation under Vision 2030, the need for robust data protection has never been more critical. With increasing reliance on cloud computing, AI, and cross-border data exchange, the Kingdom faces unprecedented opportunities and cybersecurity challenges. Inconsistent cybersecurity measures might be seen as the growing pains of a fast-growing digital economy – what matters is how policymakers and industry players respond. Given the number of cybersecurity measures being rolled out in KSA and the speed with which they are being deployed, it appears the Saudi government has recognized this area as a strategic priority, while businesses are responding with their investments in advanced security measures.

Seclore is committed to playing a pivotal role in ensuring secure third-party collaboration while helping enterprises and government entities align innovation, security, and global leadership. By implementing data-centric security, Seclore empowers Saudi Arabia to protect sensitive information without restricting digital growth. Seclore's cutting-edge solutions provide organizations with persistent data protection, automated compliance, and seamless integration, ensuring that KSA's digital assets remain secure and sovereign.

The Importance of Vision 2030

Vision 2030 is Saudi Arabia's bold roadmap for economic diversification, digital transformation, and global leadership. Saudi Arabia's social and economic evolution over the past 100 years has been rapid and, especially more recently, been defined by a leap in technological development. As one may expect in such circumstances, growth has not always been accompanied by parallel progress in security. Three robust pillars encapsulate the spirit of Vision 2030. Each represents an intricate layer of the Kingdom's roadmap to reform, symbolizing a vibrant society, a thriving economy, and an ambitious nation. Together, they echo the Crown Prince's aspirations for a nation committed to adaptability, sustainability, and global partnership.



This national initiative is designed to reduce reliance on oil revenue by fostering a thriving digital economy, strengthening public-private partnerships, and positioning the Kingdom as a leader in innovation and cybersecurity. Let's take a deeper dive into these goals and objectives.

Economic Diversification & Digital Transformation

By investing in emerging technologies such as AI, blockchain, and IoT, Saudi Arabia aims to build a knowledge-based economy where data-driven decision-making drives efficiency across industries. Rapid growth in Fintech, e-commerce, and digital banking underscores the need for strong data governance and security frameworks.

Global Cybersecurity Leadership

The Kingdom is committed to becoming a global benchmark for cybersecurity. Vision 2030's initiatives align with international best practices in data protection, fostering an environment of trust, compliance, and innovation that attracts foreign investment and partnerships.



Enhancing Public Sector Efficiency

Digital government initiatives streamline services, improve citizen engagement, and drive automation across agencies. With this rapid digitization comes the responsibility to protect sensitive government and citizen data from cyber threats and unauthorized access. Saudi Arabia invests heavily in e-government services to enhance citizen engagement and streamline administrative processes. More than 6,000 governmental services, representing 97% of services, have already been digitized. As more government functions move online, protecting sensitive citizen data becomes paramount to maintaining public trust and ensuring the efficient functioning of state institutions.

Securing Critical National Infrastructure

Industries, including energy, healthcare, and defense, are experiencing a swift digital transformation, escalating the importance of cybersecurity to protect national security and uphold economic robustness. Saudi Arabia takes this matter seriously, planning rigorously to position itself as a leading example of a forward-thinking 21st-century society through the digital revolution. This vision is well-illustrated by the ultra-modern design principles underlying monumental projects such as NEOM, including sub-projects like Oxagon, Sindalah, and Trojena. These environments, founded on advanced cyber-physical systems and AI-enabled technologies, will present many potential weaknesses. Therefore, implementing rigorous cybersecurity measures is paramount to maintaining crucial systems' integrity and preserving public safety.

“Cybersecurity is a cornerstone of Vision 2030, ensuring that our digital transformation is built on a foundation of trust and resilience.”

-Dr. Mansour Al-Qahtani, National Cybersecurity Authority

Why is KSA Data Sovereignty Important?

As Saudi Arabia ambitiously charts its course toward Vision 2030, the Kingdom has introduced robust data sovereignty measures to safeguard its digital assets and citizens and ensure economic resilience. Data sovereignty is a key pillar of Saudi Arabia's digital transformation strategy given it ensures that sensitive information remains under the control of the Kingdom's regulatory authorities. As Saudi Arabia strengthens its global economic ties, securing national data assets is essential for maintaining sovereignty, regulatory compliance, and financial resilience. Let's first talk about the reasons for enforcement.

Key Reasons for Data Sovereignty Enforcement in KSA

National Security and Economic Stability

Protecting sensitive national data prevents cyber threats that could disrupt financial markets, critical infrastructure, and government operations. A breach involving key Saudi enterprises could have severe economic consequences, undermining trust in the country's digital economy.

Regulatory Compliance and Legal Protection

Saudi Arabia's Personal Data Protection Law (PDPL) and National Cybersecurity Authority (NCA) guidelines mandate stringent controls to ensure that personal and enterprise data remain secure within national borders. Failure to comply with these regulations can lead to significant fines, reputational risks, and operational disruptions.

Balancing Data Sovereignty with Economic Growth

The Saudi Data & AI Authority (SDAIA) has the opportunity to create a regulatory environment that protects data privacy while supporting the Kingdom's economic growth. One practical approach could be introducing tiered compliance obligations based on the size and resources of the organisation. Large, well resourced multinational corporations could be required to adhere to more complex safeguards like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), while smaller entities might benefit from simpler, less resource-intensive mechanisms.

Further, regional harmonisation of data transfer standards within the Red Sea area could reduce the compliance burden on businesses that operate across borders. By working with neighboring countries to align on data privacy standards, Saudi Arabia could establish a regional data privacy framework that enables smoother cross-border operations without compromising individual privacy rights.



Metrics of Consequence: KSA



Ransomware

12%

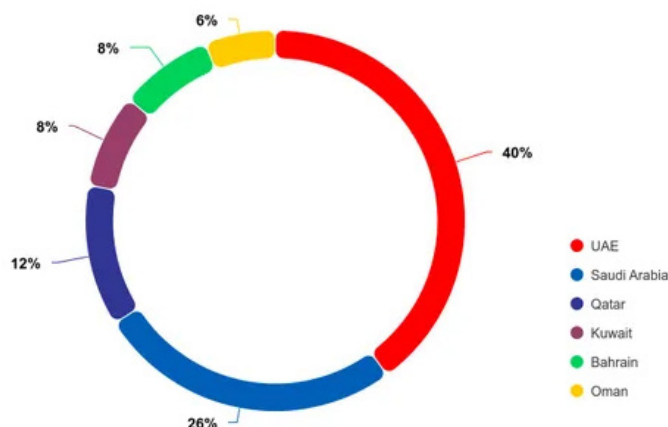
increase in malware identified 2023 vs 2024



Phishing Attempts

15%

increase in phishing identified 2023 vs 2024



These attacks are not only becoming more frequent but also more sophisticated, targeting sensitive sectors critical to the nation's economy.

Gen AI

97%

97% of respondents in KSA agree that generative AI will help their organisation develop new lines of business within the next three years (Trend Micro Annual Cybersecurity Report)

Venture Capital

#1

The Kingdom is the region's (MENA) number one destination for venture capital, capturing more than 40% of the total in 2024 with 178 deals.

The Risks of Not Protecting Saudi Arabia's Data Sovereignty

If Saudi Arabia does not enforce strict data sovereignty policies, it could face serious consequences that threaten its economic growth, national security, and international standing:

1. **Increased Cyber Threats:** Without stringent data security measures, Saudi businesses and government institutions could become prime targets for cybercriminals, foreign espionage, and ransomware attacks, leading to data leaks, service disruptions, and loss of sensitive information.
2. **Loss of Control Over Critical Data:** If national data is stored and processed outside Saudi jurisdiction, it could be subject to foreign regulations, potentially compromising state secrets, intellectual property, and personal citizen information.

By prioritizing data sovereignty, Saudi Arabia can accelerate its digital transformation while mitigating risks associated with unauthorized data access, cyber espionage, and compliance violations.



Secure 2030: Mission & Vision

Empowering Saudi Arabia's Digital Future with Uncompromising Data Security

As Saudi Arabia advances toward a technology-driven economy under Vision 2030, digital transformation is unlocking new opportunities for innovation, economic growth, and global leadership. Yet, as businesses and government entities accelerate their adoption of AI, cloud computing, and smart technologies, the need for data sovereignty, security, and compliance has never been greater.

At Seclore, we believe that true digital progress is built on trust. Our Secure 2030 initiative is a commitment to safeguarding Saudi Arabia's digital ambitions by ensuring that sensitive data remains protected, controlled, and compliant—no matter where it travels.

Through persistent, data-centric security and secure third-party collaboration, we empower Saudi enterprises, government institutions, and critical infrastructure to innovate with confidence, embrace AI securely, and maintain full control over their digital assets.

Our mission is to secure Saudi Arabia's future by enabling organizations to thrive in a digitally connected world—without compromising security, privacy, or sovereignty.

Vision

The digital revolution is no solitary pursuit; it calls for a confluence of diverse streams of innovation, expertise, and resources. Saudi Arabia's Vision 2030 embodies this spirit of collective ambition, leveraging partnerships and collaboration to spearhead a transformative journey into the digital era. Recognizing that the expertise of international partners alongside vigorous private sector participation are the cornerstones of its ambitious pathway, Secure 2030 provides the cybersecurity foundation needed to protect and accelerate this transformation.

Why Secure 2030?

Secure 2030 is designed to address the most pressing cybersecurity challenges facing Saudi Arabia's digital economy. It is a data-centric security framework that ensures sensitive information remains protected wherever it travels, providing persistent security, compliance, and risk mitigation.

- **Enable Compliance with Vision 2030's Digital Initiatives:** Align with Saudi regulations such as PDPL, NCA, and SAMA frameworks.
- **Ensure Data Sovereignty:** Protect and control sensitive national and enterprise data within Saudi Arabia's borders.
- **Strengthen Cyber Resilience:** Implement Zero Trust data security strategies that mitigate threats from cybercrime, espionage, and insider risks.
- **Foster Global Collaboration:** Support Saudi Arabia's vision of an interconnected digital economy while maintaining robust security measures.
- **Empower Enterprises with Secure AI & Cloud Adoption:** Provide a secure foundation for AI-driven innovation and cloud transformation.

Secure 2030 Pillars

Secure 2030 is built on five key pillars that align with Vision 2030's objectives:



Data-Centric Security

In today's interconnected digital landscape, traditional perimeter-based security is no longer enough. Secure 2030 champions persistent, data-centric protection, ensuring that sensitive information remains secure even beyond organizational boundaries—whether stored on-premises, in the cloud, or shared with third parties. Through policy-driven controls, enterprises and government entities can define who can access, modify, and share data, ensuring compliance and minimizing risk. By embedding security directly into the data itself, organizations can confidently collaborate and innovate without compromising control or confidentiality.



Regulatory & Compliance Readiness

With Saudi Arabia's Personal Data Protection Law (PDPL) and National Cybersecurity Authority (NCA) guidelines setting strict mandates for data governance, compliance has become a critical priority. Secure 2030 aligns with Vision 2030 advocates for full regulatory alignment, providing automated compliance enforcement for industries such as finance, healthcare, energy, and government agencies. Organizations can streamline data protection measures, meet audit requirements and reduce the risk of penalties by integrating with security policies meeting the requirements of regulatory frameworks.



Cyber Resilience & Threat Mitigation

As cyber threats become increasingly sophisticated, organizations need to adopt a proactive, Zero Trust approach to data security. Secure 2030 endorses advanced threat intelligence and real-time risk assessment tools, enabling enterprises to detect and mitigate cyber risks before they escalate into breaches. By enforcing Zero Trust principles, organizations can ensure that only verified users and devices can access sensitive information, reducing insider threats and unauthorized exposure. With continuous monitoring and automated security responses, Secure 2030 will help Saudi businesses maintain operational resilience and protect their most valuable digital assets.



Third-Party & Cross-Border Security

As Saudi enterprises expand their global partnerships and digital supply chains, ensuring secure third-party collaboration is crucial. Secure 2030 advocates for granular data controls, allowing organizations to define access levels, expiration policies, and usage restrictions for shared data—even when working with external vendors, partners, or international subsidiaries. These adaptive security controls enable data sovereignty and compliant cross-border data transfers, ensuring that Saudi enterprises remain in control of their data while meeting national and international cybersecurity regulations.



AI-Driven Digital Transformation

AI and cloud technologies are at the heart of Saudi Arabia's digital transformation. Secure 2030 recognises that AI adoption is essential for business and supports providing organizations with a framework to protect sensitive data within AI models and cloud environments. By embedding data security into AI workflows, enterprises can leverage AI-powered automation and analytics while ensuring compliance with Saudi data laws. Additionally, Secure 2030 facilitates secure cloud migration, allowing businesses to expand their digital services without exposing sensitive information to unauthorized risks.

Who Benefits from Secure 2030?

Secure 2030 is tailored to support government agencies, financial institutions, healthcare providers, energy companies, and critical infrastructure operators in Saudi Arabia. Ideal partners for the Secure 2030 initiative include organizations in the following industries:

- **Government & Public Sector:** Enabling secure e-Government services while ensuring citizen data protection.
- **Banking & Finance:** Ensuring compliance with SAMA cybersecurity frameworks and preventing financial data breaches.
- **Healthcare:** Securing electronic health records (EHRs) and enabling safe patient data exchange.
- **Energy & Infrastructure:** Protecting critical national resources from cyber threats and industrial espionage.
- **Enterprises & Corporations:** Empowering businesses with secure AI, cloud, and digital transformation strategies.

The Role of International Collaboration

Global alliances play a pivotal role in Saudi's overarching game plan, leveraging the immense technological strength of worldwide giants to facilitate a knowledge and innovation transfer. These synergies aid in establishing an environment primed for tech progress, securing Saudi Arabia's position at the cutting-edge of the digital revolution. They go beyond just enhancing capabilities; they are transformative, converting ambitions into concrete reality.

Seclore's Commitment to Saudi Arabia

Seclore is dedicated to supporting Saudi Arabia's Vision 2030 by providing cutting-edge data-centric security solutions that enable organizations to innovate with confidence. Through Secure 2030, Seclore ensures that Saudi businesses and government entities can embrace digital transformation without compromising on security or compliance.

Our Secure 2030 Commitment

- **Localized Data Protection:** Seclore supports the development of Saudi Arabia's cybersecurity ecosystem, ensuring that data sovereignty remains a top priority for businesses and government entities.
- **Strategic Partnerships:** We collaborate with government regulators, private enterprises, and global technology leaders to foster a secure and compliant digital environment.
- **Innovation & Continuous Advancement:** Seclore invests in AI-driven security solutions, automated compliance frameworks, and secure cloud adoption strategies that align with Saudi Arabia's long-term vision.
- **Capacity Building & Skill Development:** By offering training programs, cybersecurity workshops, and knowledge-sharing initiatives, Seclore empowers Saudi businesses and institutions to strengthen their security posture.
- **Resilient Digital Economy:** We work alongside stakeholders to fortify Saudi Arabia's digital economy, ensuring that organizations can operate efficiently while remaining secure, compliant, and globally competitive.

A harmonised approach between the government and the private sector is instrumental for achieving Vision 2030's goals. By fostering an environment conducive to private sector investment and participation, Saudi Arabia is setting the scene for accelerated progress and groundbreaking developments. These public-private partnerships (PPPs) are pivotal to delivering substantial infrastructural reforms and digital services that will ripple across the economy and society at large.

Partnership Type	Goals	Examples
Technology	Drive digital transformation, AI adoption, cybersecurity, and smart city initiatives.	Seclore, Google Cloud, Skyhigh, Symantec, NEOM + Oracle, Cisco, etc.
Public Sector	Drive infrastructure development, policy reforms, and economic planning.	Ministry of Investment + Foreign Firms – Facilitating foreign business operations. Giga Projects (NEOM, Red Sea Project) + Government Entities – Coordinating smart infrastructure. KACST + International Research Institutions – Advancing innovation.
Private Sector	Boost foreign direct investment (FDI), support SMEs, and diversify the economy.	PIF (Public Investment Fund) + Global Investors, Saudi Aramco + Local SMEs, Lucid Motors + Saudi Government.
Public-Private (PP)	Blend public funding with private sector innovation to build mega-projects.	Metro Riyadh (Government + Private Firms) – Building smart mobility solutions. Healthcare PPPs (Ministry of Health + Private Hospitals) – Modernizing healthcare.
Financial & Investment	Attract global investors and create alternative income streams beyond oil.	PIF + BlackRock – Co-developing financial projects. Saudi Tadawul + International Stock Exchanges – Boosting capital market integration.
Education & Research	Upskill the workforce and drive innovation.	KAUST (King Abdullah University of Science and Technology) + MIT, Stanford – Advancing research. Saudi Arabia + Coursera/Udacity – Expanding digital skills training

In summary, the fusion of both international insight and domestic enterprise underpins the success of Saudi Arabia's Vision 2030. A future sculpted by such strategic partnerships and alliances heralds a new epoch for the Kingdom, one that promises to redefine its role in the world through the lens of digital mastery. The Secure 2030 initiative was conceptualized to align and support the immense security needs of Vision 2030, together transforming the Kingdom of Saudi Arabia into a global technology leader.



Conclusion & Call to Action

In an era marked by rapid technological advances, Saudi Arabia stands at the forefront of an ambitious, transformative journey. Under the astute leadership of Crown Prince Mohammed bin Salman, the Kingdom is tactically executing on Vision 2030, a blueprint designed to reshape its economy and society. The cornerstone of this sweeping reform is digital transformation – a strategic thrust envisioned to propel Saudi Arabia into a digital age of innovation, diversification, and inclusive growth. With the integration of advanced technologies into government services and the private sector, the Saudi Vision aims to transcend the nation's reliance on oil, cementing its status as a global powerhouse in the digital economy. Organizations that fail to secure their data risk non-compliance, reputational damage, and loss of business opportunities. Seclore is ready to be a strategic partner in enabling data-centric security as the Kingdom moves toward a secure and prosperous digital future.

Seclore's expertise in persistent data protection, automated policy enforcement, and regulatory compliance makes it the ideal partner for organizations aligning with Vision 2030's security and innovation goals. By adopting data-centric security solutions, enterprises and government agencies can ensure their data remains protected no matter where it travels. Saudi Arabia's data governance and cybersecurity leadership will set a global precedent, demonstrating how nations can embrace digital transformation while safeguarding their most valuable digital assets.

Join us in creating a secure and future-ready organization. Contact Seclore today to learn how we can help secure your data, ensure compliance, and drive your business forward in alignment with Saudi Arabia's Vision 2030.

About Seclore

Our mission is to safeguard sensitive information worldwide, regardless of its location. Seclore offers persistent protection and visibility for digital assets to help organizations remain secure and compliant. Our data-centric security approach ensures that only authorized individuals can access protected digital assets. With Seclore, organizations can specify who can access their data, what actions are permitted, and how long that access lasts. Trusted by Fortune 500 companies, government agencies, and critical infrastructure providers, Seclore ensures organizations can protect and control their digital assets without sacrificing seamless collaboration and data sharing.

Visit www.seclore.com for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054