Cloud

Whitepaper

Accelerating SAMA Regulatory Compliance

Through Secure, Compliant SITE Cloud Platform

Feb 2026 cloud.site.sa

Disclaimers

This document is designed to provide helpful information on the subject matter within. The recipient acknowledges and agrees that any advice, recommendations, reports, analyses, deliverables, or other material provided by Saudi Information Technology Company to the recipient are intended solely for the benefit of recipient and not any other third party. Saudi Information Technology Company made every attempt to ensure the accuracy and reliability of the information on this document. However,it assumes no responsibility for errors, omissions, misuse, misunderstanding, or inapplicability of the contents of this document. In no event shall Saudi Information Technology Company be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence or other tort, arising out of or in connection with the use of the information contained in this document.

Confidentiality

This document may contain information of a sensitive nature. This information should not be shared with anyone other than those for whom it was originally intended. No one else may disclose, distribute or otherwise use the contents of this document without the express written permission of the owner. Unauthorized use, disclosure, dissemination, duplication and/or distribution are strictly prohibited, and may be unlawful. If you receive this document in error, please immediately delete it and all copies of it from your system, destroy any hard copies of it, and notify Saudi Information Technology Company.

Copyright

The information contained in this document is the proprietary and exclusive property of Saudi Information Technology Company except as otherwise indicated. Notwithstanding its intended purpose, no part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for any purpose without the prior written permission of the Company.

Contents


Site

Executive Summary

In the Kingdom of Saudi Arabia (KSA), the Saudi Central Bank (SAMA) is the principal monetary authority dedicated to ensuring the stability and resilience of the financial sector's digital landscape.

As the Central Banking Authority, SAMA establishes and enforces a comprehensive suite of mandatory frameworks and requirements, the core frameworks are:

CSF

The SAMA Cybersecurity Framework

CRFR

The Cyber Resilience Framework and Requirements

BCM

The foundational Business Continuity Management Framework

For financial institutions, compliance with SAMA's mandates is more than a technical obligation; it is a strategic imperative that directly impacts business continuity, safeguards public trust, and influences competitive positioning within the KSA market.

Beyond these core frameworks, SAMA also mandates specific policies and controls governing the secure adoption of modern technologies.

SITE Cloud recognizes the importance of these controls and has designed its platform and services with built-in cybersecurity features to accelerate clients' compliance with the SAMA CSF and Cloud Security mandates. SITE Cloud also natively supports the resilience and availability requirements of the CRFR and BCM frameworks; helping make digital transformation and innovation smoother and more efficient.

SITE Sovereign Cloud

Is the leading sovereign cloud in the Kingdom, operating on a nationally built operating system (SITE Cloud OS) to ensure uninterrupted business continuity from Riyadh and Jeddah. Its cutting-edge self-service provisioning streamlines rapid business rollout, ensuring compliance with SAMA's cybersecurity, data residency, and regulatory frameworks.

Comprehensive support

Comprehensive SAMA compliance extends beyond technical controls. SITE offers a complete solution: SITE Advisory, Professional, and Managed Services provide expertise, tooling, and guidance for domains associated with organizational controls. This ensures you have the resources needed to address all aspects of the SAMA framework, while retaining responsibility for organizational and policy controls.

01

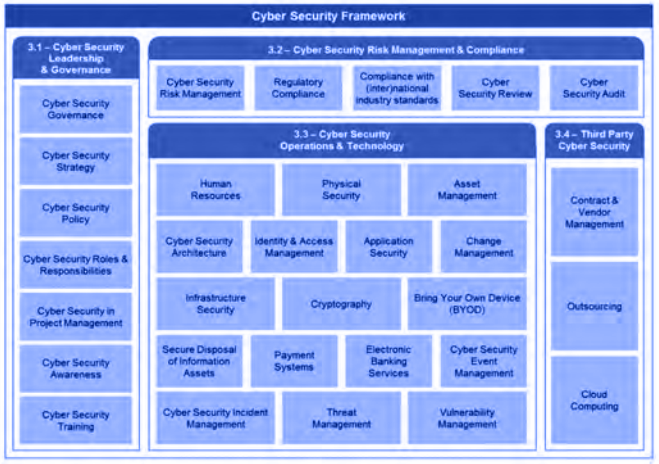
SAMA Frameworks

Understanding the Importance of the SAMA Cybersecurity Framework (CSF)

Regulatory Landscape: SAMA's Compliance Framework

The Saudi Arabian Monetary Authority (SAMA) enforces a stringent regulatory regime for financial services, including the nation's most comprehensive Cybersecurity Framework (CSF).The framework is compulsory for all banks, insurance companies, fintech, and regulated financial entities, covering:

- Data residency, requiring all data and processing to stay strictly within KSA
- Third-party risk controls and outsourcing oversight
- Robust encryption and key management
- Timely incident response and documentation
- Continuous monitoring and risk management
- Business continuity and disaster recovery



Source: SAMA – Cybersecurity Framework

Core Objectives and Domains

Enhance Resilience

Establish a robust defense posture capable of withstanding, detecting, and rapidly recovering from cyber incidents.

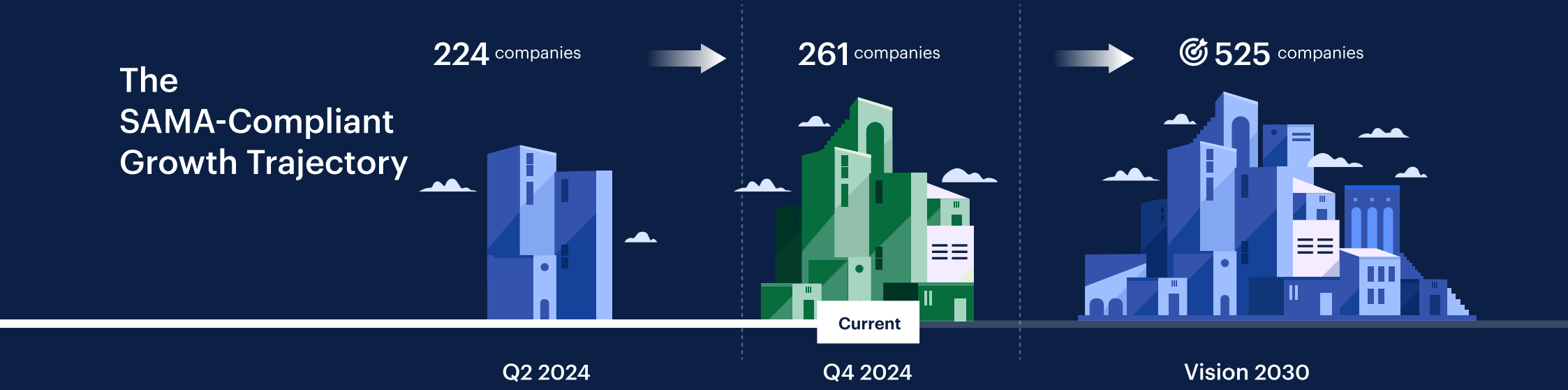
Protect Financial Stability

Safeguard critical banking and financial systems, preventing disruptions that could harm the national economy.

Promote Consistency

Create a common, unified standard for addressing cybersecurity risks across the financial sector.

The SAMA-Compliant Growth Trajectory



Source: SAMA, Financial Sector Development Program Annual Report 2024

SAMA Cybersecurity Maturity Model

The cybersecurity maturity level is measured with the help of a predefined cybersecurity maturity model. The Cybersecurity Maturity Model distinguishes 6 maturity levels (0, 1, 2, 3, 4 and 5), which are summarized in the table below. In order to achieve levels 3, 4 or 5, a Member Organization must first meet all criteria of the preceding maturity levels.

The objective of the CSF is to create an effective approach for addressing cybersecurity and managing cybersecurity risks within the financial sector. To achieve an appropriate maturity level, member organizations should operate at maturity level 3.

5. Adaptive Mature	Cybersecurity controls are subject to a continuous improvement plan, periodic measurements, evaluations, and improvement opportunities are documented.			5
4. Managed & measurable Mature	• The effectiveness of the cybersecurity controls are periodically assessed and improved when necessary.	• This periodic measurement, evaluations and opportunities for improvement are documented.		4
3. Structured & formalized Mature	• Cybersecurity controls are defined, approved and implemented in a structured and formalized way.	• The implementation of cybersecurity controls can be demonstrated.		3
2. Repeatable but informal	Controls are performed inconsistently, execution is based on informal, unwritten (but standardized) practice.			2
1. Ad hoc	• Cybersecurity controls are not defined or are only partially defined.	• Cybersecurity controls are performed in an inconsistent way.	• Cybersecurity controls are not fully defined.	1
0. Non-existent	• No documentation.	• No awareness or attention for certain cybersecurity control		0

Source: SAMA – Cybersecurity Framework

SAMA-Enabled Growth

FINTECH JOBS CREATED

7K+

Direct employment
Q2 2024

PUBLICLY TRADED COMPANIES

353

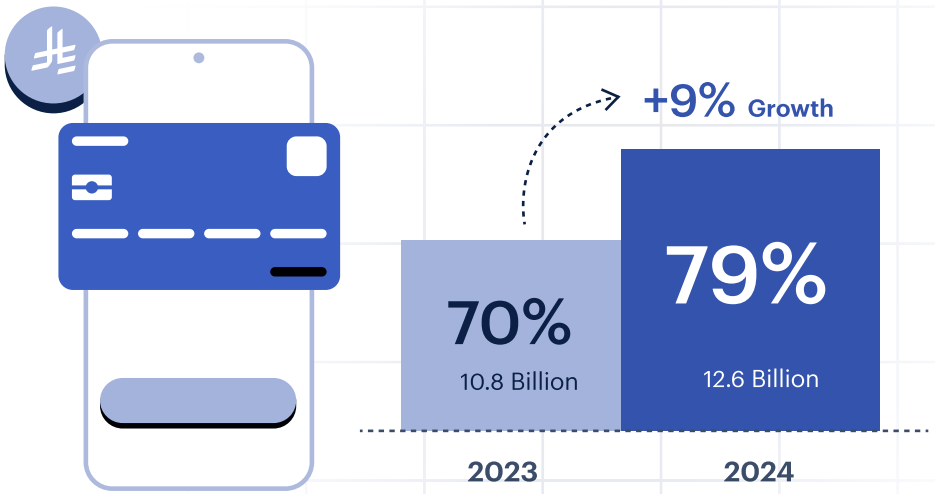
44 new in 2024

VC INVESTMENT

SAR **7.1B**

Since inception (Q2 2024)

KSA is witnessing a remarkable shift toward cashless transactions powered by SAMA's strategic initiatives



Key Insights & Impact

Exceeded Targets

261 licensed fintech companies surpassed the FSDP 2024 target, tracking toward the 2030 goal.

Digital Payment Surge

Electronic payments reached 79% of retail transactions in 2024, up 9 percentage points from 2023, driven by SAMA initiatives.

Economic Transformation

Strong regulatory support and consumer adoption are anchoring Saudi Arabia's Vision 2030 financial sector goals.

VISION رؤية 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

02

SITE Sovereign Cloud Overview

SITE Sovereign Cloud

It is the leading sovereign cloud operating within the Kingdom, designed to meet the highest standards of performance, cybersecurity, and compliance. It operates across Riyadh and Jeddah regions and is built on a nationally developed operating system (SITE Cloud OS) to support uninterrupted business continuity.

24/7

Protection through managed Security Operations Center (SOC) and Network Operations Center (NOC).

100+

Products and services across IaaS, PaaS, and SaaS to meet diverse business needs.

60+

Cybersecurity controls built into th design of SITE Cloud, aligned with local and international standards to accelerate compliance in data, cybersecurity, and information technology.

20+

Local and international certificates and awards, reflecting our strong commitment to the highest safety and quality standards.

Service Delivery Principles

- **Local operation & support**
- **Local data**
- **Local connection**
- **National Talent**

Dedicated Region

SITE Cloud Dedicated Region is an additional deployment model within the SITE Cloud portfolio, offered for banks, governments, and highly regulated organizations in Saudi Arabia.

Key Features

- **Exclusivity**: Private deployment with dedicated hardware at your location.
- **Optimized for Sensitive Data**: Ideal for mission-critical and legacy workloads.
- **OpEx Model**: Pay-as-you-go with zero upfront costs and a minimal commitment.
- **Compliance Acceleration**: Ensures data residency, auditability, predictable performance, and business continuity
- **Fully Managed**: SITE handles installation, operations, upgrades, and support.

Adopting SITE Saudi Sovereign Cloud ensures true sovereignty across all dimensions:

Data Sovereignty, ensuring data is stored, processed, and accessed in accordance with local laws and regulations

Operations Sovereignty, ensuring the control and management of cloud operations are aligned with local autonomy and oversight

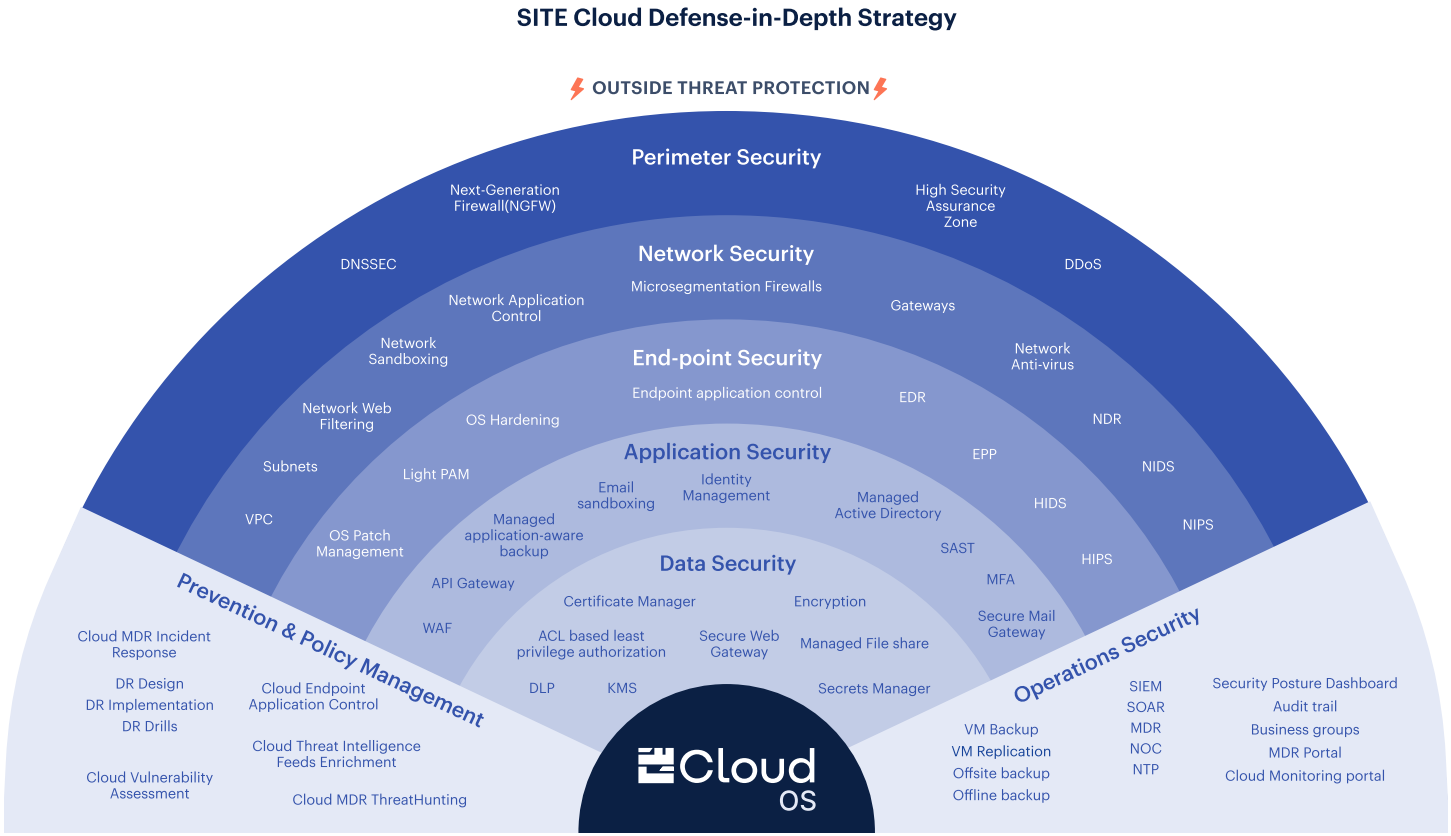
Technology Sovereignty, ensuring that the underlying technology, infrastructure, platforms, and software are governed, and controlled to reduce reliance on foreign technologies

03

Cloud

SITE Sovereign Cloud Built-in Cybersecurity Solutions

SITE Sovereign Cloud Built-in Cybersecurity



At the core our secure-first approach is our proprietary **SITE Cloud Orchestrator** (SITE Cloud OS), which enables the seamless integration of advanced cybersecurity controls and technologies.

SITE Cloud OS safeguards data and systems, simplifies compliance, and enhances cloud security management through its comprehensive cybersecurity framework

Defense-in-Depth is the implementation of multiple, overlapping cybersecurity controls to protect data and systems. Each layer presents a barrier to attackers, making it significantly harder to compromise assets. This strategy is especially critical in the cloud, where rapid deployment can introduce additional management complexity. SITE Cloud employs a Defense-in-Depth strategy that strengthens both cybersecurity and compliance.

This cybersecurity strategy empowers organizations to:

- **Ensure business continuity:**
  Redundancy, backups, and incident response ensures operational resilience.
- **Prevent unauthorized access:**
  Multi-layer authentication and network segmentation help keep systems secure.
- **Protect data confidentiality and integrity:**
  Encryption and secure configurations protect your valuable information.

01 Perimeter Security

High Security Assurance Zone (HSA):

A restricted zone for sensitive workloads or critical systems that limits public internet exposure and leverages advanced access controls, encryption, and monitoring to meet strong compliance requirements.

Cloud DDoS Protection:

Protects systems and applications from Distributed Denial-of-Service (DDoS) attacks.

Cloud DNSSEC:

Built-in DNSSEC safeguards against threats like DNS spoofing or cache poisoning, supporting secure navigation to legitimate websites and services.

Cloud Physical Perimeter Next-Generation Firewall (NGFW):

Provides robust network security and threat protection at cloud network perimeter.

REGIONAL THREAT INSIGHT *

121%

YoY increase in DDoS attack volume targeting Saudi organizations

490 Gbps

Largest DDoS attack mitigated in KSA

49%

of DDoS attacks use DNS amplification vectors

SITE CLOUD PROTECTION

- Anti-DDoS and NGFW absorb and block volumetric attacks.
- DNSSEC and secure DNS gateways prevent spoofing and amplification.
- High Security Assurance Zones isolate critical services from external threats.

THREATS MITIGATED

- Volumetric and protocol-based DDoS attacks
- DNS amplification and reflection attacks
- Perimeter reconnaissance and service disruption

Sources: Refer to the References section for detailed source citations.

02

Network Security

Cloud Micro-segmentation Firewall:
Applies zero-trust principles to limit east-west traffic between virtual machines (VMs) through firewall policies. This reduces attack surfaces, prevents lateral movement, contains breaches, and supports regulatory compliance.

Cloud Network Intrusion Detection & Prevention Systems (NIDS/NIPS):
Detects and prevents network-based attacks by monitoring traffic for suspicious patterns and known signatures

Cloud Network Intrusion Detection System (NIDS):
Cloud NIDS detects known threats by monitoring network traffic for suspicious patterns and comparing it against a database of known attack signatures.

Cloud Network Detection & Response (NDR):
Detects and responds to known and unknown threats using signature detection, behavioral analysis, machine learning, and anomaly detection.

Cloud Network Web Filtering:
Controls and filters web content to support security policies.

Cloud Network Anti-Virus (AV):
Scans and protects systems and devices from viruses, malware, and other malicious threats.

Cloud Network Sandboxing:
An isolated environment for analyzing suspicious network traffic.

Cloud Subnets:
Enable isolation of device groups to enhance security segmentation.

Cloud Application Control:
Identifies applications at Layer 7 and protects your network by controlling app usage

Cloud VPC:
Built-in Standard Security Assurance (SSA) and High Security Assurance (HSA) Virtual Private Clouds (VPCs) are protected by multiple firewalls (physical, micro-segmentation and WAF) for internet-facing and non-internet facing applications.

Secure GSN Gateway:
A managed, compliant gateway providing isolated, audited connectivity between workloads in SITE cloud and the Saudi Government Secure Network (GSN), without exposure to the public internet.

Cloud Private Connect Gateway:
Ensures a controlled and secure connection between a VDC and on-premises environments.

Cloud Intra-VPC Gateway:
Provides low-latency, highly secured private connectivity between SSA and HSA VPCs.

Cloud HTTP Gateway:
Provides a uni-directional HTTP flow from instances in HSA VPC to an authorized list of web servers, enabling package downloads and updates.

Cloud Shared Area Gateway:
Allows optional routing of traffic to and from the Cloud Shared Area Network.

Cloud Internet Gateway:
Allows optional routing of traffic to and from the internet (for SSA VPC workloads).

REGIONAL THREAT INSIGHTS

42.9%
Of incidents originate from public-facing application exposure

Lateral movement observed in >50% of incident response cases

43%
of breaches involve valid account abuse

SITE CLOUD PROTECTION

- Micro-segmentation firewalls stop lateral movement across workloads.
- Network IDS/IPS and NDR detect suspicious internal traffic.
- Secure gateways and subnet isolation restrict network access paths.

THREATS MITIGATED:

- Lateral movement within cloud environments
- Credential replay and internal pivoting
- Network-borne malware propagation

Sources: Refer to the References section for detailed source citations.

03 Endpoint Security

Cloud Endpoint Protection - Anti-Malware (EPP):

Protects endpoints against malware and other malicious threats.

Cloud Endpoint Detection and Response (EDR):

Detects and responds to advanced threats and suspicious activities on endpoints.

Cloud OS Hardening:

VMs are fortified with robust security controls to enforce secure configurations and align with best practices to protect against threats and ensure compliance.

OS Patch Management:

Internal repository for operating system software packages and updates, enabling controlled access and efficient distribution.

Cloud Endpoint Application Control:

Controls and monitors endpoint applications to support secure and compliant operations.

Light PAM:

Managed privileged access monitoring and control to reduce the risk of unauthorized activity and support compliance requirements.

Cloud Host Intrusion Detection & Prevention Systems (HIDS/HIPS):

Host-based automated detection and protection that continuously monitors for & responds to intrusions, malware, and other unauthorized activities in real-time to support secure and compliant operation.

REGIONAL THREAT INSIGHTS

57%

Of ransomware attacks use PowerShell or LOLBins

Ransomware, RATs, and cryptominers are top endpoint threats

94%

Of ransomware incidents involve data exfiltration

SITE CLOUD PROTECTION

- EPP and EDR detect malware and abnormal endpoint behavior.
- OS hardening and endpoint application control limit attack surface.
- HIDS/HIPS block malicious host-level activity.

THREATS MITIGATED

- Fileless malware and privilege escalation
- Ransomware execution and persistence
- Endpoint-based data exfiltration

Sources: Refer to the References section for detailed source citations.

04 Application Security

Cloud WAF:

Web application firewall that protects against common exploits and vulnerabilities.

Cloud Identity Management:

Controls and manages user identities and access controls.

SAST:

Cloud-native scanning of application source code to identify and remediate vulnerabilities early in the development lifecycle.

API Gateway:

Fully managed, serverless gateway that securely exposes and routes APIs, handles authentication, traffic management, and scaling automatically

Secure Mail Gateway:

A secure gateway that filters and scans incoming and outgoing emails for malicious content.

Cloud Email Sandboxing:

An isolated environment for analyzing potentially harmful emails.

Managed Application-Aware Backup:

Ensures secure, reliable, and automated data backups to prevent data loss and facilitate rapid recovery.

Managed Active Directory (AD):

Secure and efficient directory services, which including user management, authentication, and access control.

Cloud Multi-Factor Authentication (MFA):

A security layer that requires two or more distinct forms of identification to access a system.

REGIONAL THREAT INSIGHTS

63%

of web threats are malware-based

12.68%

of all emails classified as malicious

Public-facing apps are the #1 initial access vector

SITE CLOUD PROTECTION

- WAF blocks exploits on web applications.
- API Gateway secures APIs with authentication and traffic inspection.
- Secure Web and Mail Gateways prevent phishing and malware delivery.
- Identity Management with MFA controls application access.

THREATS MITIGATED

- Web exploitation and API abuse
- Phishing and business email compromise (BEC)
- Unauthorized application access

Sources: Refer to the References section for detailed source citations.

05

Data Security

Cloud Virtual Machine Storage Encryption:

Protects data at rest by encrypting VM disk files and configuration data using cryptographic keys

Cloud KMS:

Secure and compliant key management and cryptographic services for encrypting and protecting sensitive data.

Cloud Certificate Manager:

Enables uploading, deploying, and managing digital certificates with timely updates to support compliance.

Secrets Manager:

Securely stores, manages, and rotates sensitive credentials, API keys, and secrets, reducing the risk of unauthorized access.

Secure Web Gateway:

Monitors and controls web traffic, protecting users from malicious sites, enforcing policies, and supporting compliance requirements.

Data Loss Prevention (DLP):

Monitors, detects, and protects sensitive data within your environment, reducing the risk of data leaks and helping you meet compliance requirements.

ACL-based least-privilege authorization:

Enforces granular access control by granting users only the minimum necessary permissions through Access Control Lists.

Managed File Share:

Secure, efficient, and collaborative file sharing solution for streamlined workflow management.

REGIONAL THREAT INSIGHTS

52%

Of breaches expose customer PII

SAR 15M–19M

Average cloud breach cost

Credential leaks and stealer logs prevalent in MEA

SITE CLOUD PROTECTION

- VM storage encryption and KMS secure data at rest and in transit.
- Secrets Manager protects and rotates credentials.
- DLP and secure file sharing monitor sensitive data movement.

THREATS MITIGATED

- Data leakage and unauthorized access
- Credential theft and secrets exposure
- Regulatory and compliance violations

Sources: Refer to the References section for detailed source citations.

06

Operations Security

Security Posture Dashboard:

Continuous visibility into your environment's cybersecurity posture, highlighting risks, compliance gaps, and recommended actions to enhance protection.

Cloud SIEM:

Security solution for centralized event log analysis, threat detection, and incident response.

Cloud SOAR:

An advanced platform for Security Orchestration, Automation, and Response, streamlining and enhancing your cloud security operations.

Cloud MDR - Managed Detection and Response:

Security operations center for cloud environments providing proactive and comprehensive threat detection and response for robust cybersecurity.

Cloud NOC - Network Operations Center:

Centralized hub for monitoring and managing network infrastructure to ensure optimal performance and security.

Cloud Monitoring Portal:

A platform for monitoring cloud infrastructure resources and application utilization.

Cloud Network Time (NTP) System:

Time synchronization across the environment for consistent and coordination.

Cloud Provider Portal:

Web-based user interface for managing SITE cloud resources.

Cloud MDR Portal:

Easy-to-use platform for monitoring and interacting with the SITE MDR Service.

Business Groups:

Organize workloads into flexible, dynamic groups, allowing for robust and effective access control management.

Virtual Machine Backup:

Create recoverable copies of data to restore from loss, damage, or accidental deletion.

Virtual Machine Replication:

Provides replication of virtual machines for high availability and disaster recovery.

Offline Backup:

Offline backup involves storing data on physical media disconnected from the network, ensuring protection against cyber threats and data loss.

Offsite Backup:

Offsite backup stores data in multiple regions, ensuring data protection and recovery in case of local disasters or failures.

Cloud Audit Trail:

Records events, activities, user and system actions performed in the cloud environment.

REGIONAL THREAT INSIGHTS

64 days

Mean Time to Identify breach

194 days

Mean Time to Contain breach

SITE CLOUD PROTECTION

- SIEM aggregates logs for centralized threat visibility.
- SOAR and MDR automate detection and response.
- Dashboards, NOC monitoring, and audit trails ensure operational oversight.

THREATS MITIGATED

- Undetected intrusions and long dwell times
- Slow or ineffective incident response
- Repeated or escalated breaches

Sources: Refer to the References section for detailed source citations.

07

Prevention & Policy Management

Disaster Recovery Design, Implementation, Drills:
Services to design, implement, and drill for resilient recovery of data and systems during critical incidents.

Cloud MDR Threat Hunting:
Expert-lead search for hidden threats within instances and networks to reduce risk and enhance security.

Cloud Vulnerability Assessment:
Regular vulnerability scans for internet-exposed resources with alerts, recommendations and mitigation steps for identified vulnerabilities.

Cloud Threat Intelligence Feeds Enrichment:
Threat intelligence collected, correlated, and enriched from multiple sources, including Saudi's Local TI feeds, to improve detection and mitigation.

Cloud MDR Incident Response:
Monitoring, detection, and response services for security incidents in cloud environments.

Cloud Endpoint Application Control:
Controls and monitors endpoint applications to support secure and compliant operations.

REGIONAL THREAT INSIGHTS

51%
Of organizations cite misconfiguration as top cloud risk

Human error and weak policy enforcement drive breaches

DR readiness varies significantly across MEA

SITE CLOUD PROTECTION

- Endpoint and application controls enforce security policies.
- Cloud vulnerability assessments identify misconfigurations.
- Built-in backup and DR services enable rapid recovery.

THREATS MITIGATED

- Cloud misconfiguration exposure
- Compliance and audit failures
- Prolonged downtime after attacks

Sources: Refer to the References section for detailed source citations.

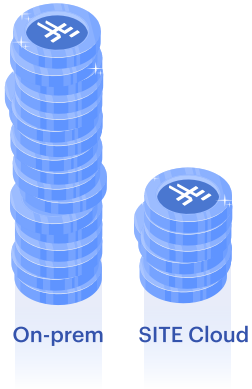
Key Benefits with SITE Cloud Built-Ins

Reduced Total Cost of Ownership (TCO)

Enterprises can save

Up to 35%

on 3-year TCO by moving workloads to SITE Sovereign Cloud.



Reduced Capital Expenditure (CapEx):

- **No Hardware Investments:** Avoid dedicated security appliances (e.g., firewalls, IDS, or SIEM) and related refresh cycles.
- **No Software Licensing Fees:** Security tools are built-in, eliminating upfront purchase and licensing costs.

Reduced Operational Expenditure (OpEx):

- **Lower Management & Maintenance:** SITE Cloud handles all security maintenance, updates, and patching.
- **Reduced Staffing & Training:** Less dependence on specialized staff for day-to-day operations and tool integration.
- **Lower Energy & Space:** Reduce footprint and power requirements compared to on-premises security hardware.

Improved Time to Value

- **Faster deployment:** Secure environments can be deployed quickly without lengthy procurement and implementation cycles.
- **Increased agility:** Built-in security enables teams to focus on core business outcomes rather than the security infrastructure management.

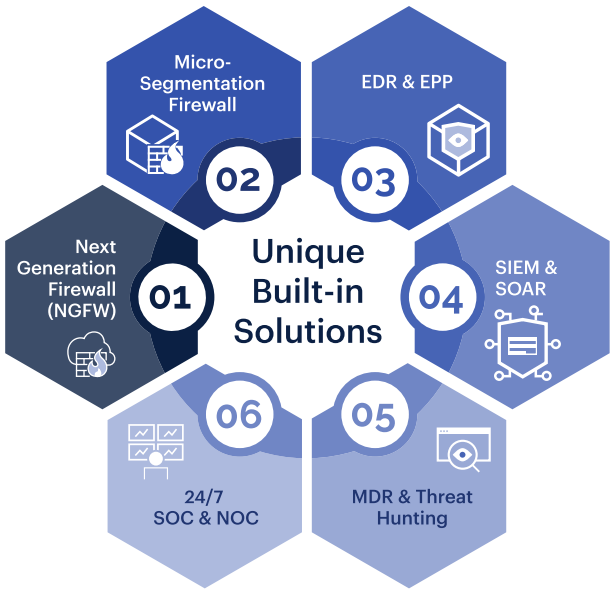
Both SITE Sovereign Cloud and Dedicated Region offerings include the built-in cybersecurity stack, while also delivering cost efficiency and faster time-to-value.

Enhanced Security Posture

- **Proactive security:** SITE Cloud leverages threat intelligence and automation to proactively identify and mitigate threats.
- **Faster incident response:** Integrated cybersecurity tools enable faster detection and response to security incidents.

Multi-Layered Protection

SITE Cloud provides a comprehensive, multi-layered cybersecurity suite (Defense-in-Depth). This multi-layered approach ensures continuous asset protection, minimizes the risk of a successful attack, and contributes to strong compliance.



04

Mapping Guide

Mapping of SITE Cloud Security Products & Services to SAMA Technical Controls

How SITE Cloud Supports SAMA Technical Controls (CSF, CRFR, BCM)?

There are six key consolidated domains across SAMA's CSF, CRFR, and BCM frameworks for cybersecurity compliance: Cybersecurity Leadership & Governance, Cybersecurity Risk Management & Compliance, Cybersecurity Operations & Technology, Third-Party Cybersecurity, Resilience, and Business Continuity requirements.

SITE Cloud provides robust, built-on, and adaptable pay-as-you-go products that directly support numerous technical controls within four critical domains: Cybersecurity Operations & Technology, Third-party Cybersecurity, Resilience, and Business Continuity.

To ensure comprehensive SAMA compliance, SITE Advisory, Professional and Managed services offer expert advisory, tooling, and guidance for the remaining domains and specific sub-domains within Cybersecurity Operations & Technology.

SITE Cloud operates under a shared responsibility model. Clients remain responsible for implementing organizational and governance controls, while SITE Cloud focuses on delivering technical controls within Cybersecurity Operations & Technology, Third-Party Cybersecurity, Resilience, and Business Continuity while providing expert support for other areas. This full value-chain support enables clients to:

- **Simplify compliance efforts.**
- **Streamline the implementation of controls within supported domains.**
- **Significantly strengthen the cybersecurity posture and related risks.**

SAMA DOMAINS & SUBDOMAINS ACROSS CSF, CRF, BCM

1. Cybersecurity Leadership & Governance
2. Cybersecurity Risk Management & Compliance
3. Third Party Cybersecurity
4. Cybersecurity Operations & Technology
Human Resources
Physical Security
Asset Management
Cybersecurity Architecture
Identity & Access Management
Application Security
Change Management
Infrastructure Security
Cryptography
Bring Your Own Device (BYOD)
Secure Disposal of Information Assets
Payment Systems
Electronic Banking Services
Cybersecurity Event Management
Cybersecurity Incident Management
Threat Management
Vulnerability Management
5. Resilience
6. Business Continuity Management

Supported by SITE Cloud

Supported by SITE Advisory, Professional & Managed services

1. Mapping of SITE Cloud Cybersecurity Products to SAMA Technical Controls

Mapping SITE Cloud built-ins to SAMA CSF, CRFR, BCM technical controls under Cybersecurity Operations & Technology and Cybersecurity resilience

1. Physical Security

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Physical Entry Controls 2. Monitoring and Surveillance 3. Environmental Protection

2. Asset Management

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Asset Labeling 2. Unique Resource Identifier 3. Cloud Provider Portal

3. Cybersecurity Architecture

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Secure Landing Zone
2. Business Groups
3. Standard Security Assurance (SSA) Zone
4. High Security Assurance (HSA) Zone
5. Cloud End-Point Protection (EPP)
6. Cloud End-point Detection and Response (EDR)
7. Cloud Audit Trail
8. Cloud SIEM
9. Cloud MDR
10. 24/7 SOC & NOC

4. Identity and Access Management

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Identity Management
2. Cloud MFA
3. Cloud SSO
4. Cloud Audit trail
5. ACL-based least-privilege authorization

On-demand Products & Services:

1. Light PAM

5. Application Security

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. High Security Assurance (HSA) Zone
2. Standard Security Assurance (SSA) Zone
3. Cloud WAF
4. ACL-based least-privilege authorization

On-demand Products & Services:

1. VM backup
2. Database backup
3. Managed File Share
4. Offline backup
5. Offsite backup
6. Managed application-aware backup

6. Infrastructure Security

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Cloud Physical Perimeter NGFW
2. Cloud Micro-segmentation Firewall
3. Cloud NIPS
4. Cloud NIDS
5. Cloud Network Application Control
6. Cloud Network Web Filtering
7. Cloud Network Anti-virus
8. Cloud Network Detection & Response
9. Cloud Network sandboxing
10. Cloud DDoS protection
11. Cloud HIDS
12. Cloud HIPS
13. Cloud VM Storage Encryption
14. Cloud KMS
15. Cloud MFA
16. Secure Remote Access
17. Cloud WAF
18. Cloud OS Hardening
19. Standard Security Assurance (SSA) Zone
20. High Security Assurance (HSA) Zone
21. Cloud Subnets
22. Cloud Private Connect Gateway
23. Cloud HTTP Gateway
24. Cloud Internet Gateway
25. Cloud Intra-VPC Gateway
26. Cloud Shared Area Gateway
27. Cloud Certificate Manager
28. ACL-based least-privilege authorization
29. Business Groups
30. Cloud NTP
31. Cloud Private Mirror Repository
32. Cloud WSUS server

On-demand Products & Services:

1. VM backup
2. Database backup
3. Data Loss Prevention (DLP)
3. Offline backup
4. Offsite backup
5. Managed application-aware backup

7. Cryptography

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Cloud HSM
2. Cloud VM Storage Encryption
3. Cloud KMS

8. Cybersecurity Event Management

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Cloud SIEM
2. Cloud SOAR
3. Cloud EDR
4. Cloud Monitoring Portal
5. Cloud MDR
6. Cloud SOC & NOC
7. Cloud Threat Intelligence Feeds Enrichment

On-demand Products & Services:

1. Light PAM

9. Secure Disposal of Information Assets

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Secure Data Erasure
2. Cloud VM Storage Encryption
3. Cloud KMS

10. Cybersecurity Incident Management

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Cloud SIEM
2. Cloud SOAR
3. Cloud Threat Intelligence Feeds Enrichment
4. Cloud MDR
5. Cloud SOC & NOC
6. Cloud MDR Portal

11. Cybersecurity Threat Management

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Cloud SIEM
2. Cloud SOAR
3. Cloud Threat Intelligence Feeds Enrichment
4. Cloud MDR
5. Cloud SOC & NOC
6. Cloud MDR Portal

12. Vulnerability Management

CSF ✓ CRFR ✓ BCM –

Built-In Products & Services (free-of-charge):

1. Cloud Vulnerability Assessment
2. Cloud Threat Intelligence Feeds Enrichment
3. Cloud WSUS Server
4. Cloud Private Mirror Repository
5. Cloud EDR
6. Cloud MDR
7. Cloud SOC & NOC

13. Resilience, Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

CSF – CRFR ✓ BCM ✓

Built-In Products & Services (free-of-charge):

1. Cloud MDR
2. Dual Regions with Tier IV Data Centers

On-demand Products & Services:

1. VM Backup
2. VM Replication
3. DR Design, Implementation & Drills
4. Offline Backup
5. Offsite Backup
6. Managed application-aware backup

2. Third Party Cybersecurity

SITE Cloud enables customers to perform due diligence, manage outsourcing and third-party risks, protect data confidentiality, and maintain appropriate oversight and audit rights. This helps regulated entities demonstrate that cybersecurity risks related to third-party and cloud service providers are properly managed in line with SAMA expectations.

1. Contract and Vendor Management

CSF ✓ CRFR – BCM –

SITE Cloud establishes, implements and maintains the following:

1. Baseline Cybersecurity requirements
2. Cybersecurity Audits
3. Cyber Risk Assessment Program
4. Contract & SLAs
5. Cloud Services & Billing Portal
6. Cloud Compliance Attestation

2. Outsourcing

CSF ✓ CRFR – BCM –

SITE Cloud establishes, implements and maintains the following:

1. Dedicated Service Delivery Teams
2. Contract & SLAs
3. Cybersecurity Audits
4. Cloud Compliance Attestation

3. Cloud Computing

CSF ✓ CRFR – BCM –

SITE Cloud establishes, implements and maintains the following:

1. Cyber Risk Assessment Program
2. Data Sovereignty
3. Data Segregation Infrastructure,
4. Application & Data Security controls
5. Secure Data Erasure
6. Cybersecurity Audits
7. Business Continuity & Disaster Recovery

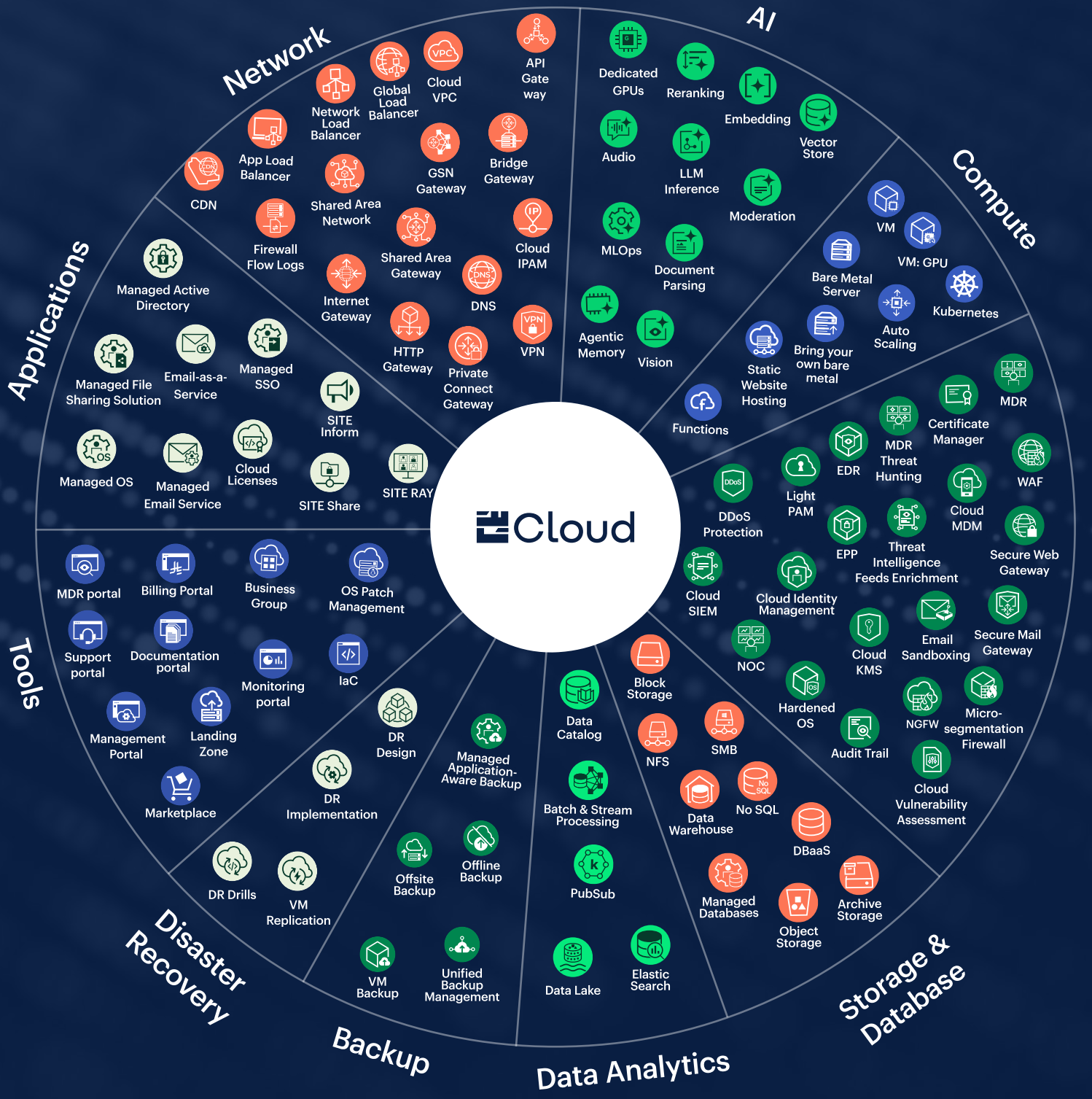
SITE's Commitment to Compliance and Standards

SITE Cloud combines a Saudi-centric approach with comprehensive multi-layered cybersecurity, extensive product offerings, and dedicated local support, providing a cloud solution that meets the highest standards of performance and compliance.

Conclusion

Achieving robust cybersecurity compliance with the SAMA's CSF, CRFR, and BCM frameworks and requirements demands a multifaceted strategy. SITE Cloud provides a critical foundation, simplifying compliance with built-in security for Cybersecurity Defense and Resilience, while our comprehensive suite of SITE Advisory, Professional, and Managed services ensures expert guidance and support for all other domains and key sub-domains. This holistic approach empowers organizations to not only meet compliance requirements but also strengthen their overall security posture, reduce TCO, improve time to value, and focus on core business objectives. While client-specific controls remain essential in certain areas, SITE Cloud delivers a powerful and cost-effective solution for building a secure, compliant, and business-driven cloud environment.

Beyond Cybersecurity



References

- SAMA – Cybersecurity Framework
  https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf
- SAMA – Cyber Resilience Fundamental Requirements (CRFR)
  https://rulebook.sama.gov.sa/en/cyber-resilience-fundamental-requirements-crfr-1
- SAMA – Business Continuity Management Framework
  https://rulebook.sama.gov.sa/en/business-continuity-management-framework-1
- Annual Report for the Financial Sector Development Program 2024
  https://www.sama.gov.sa/en-US/Documents/Financial_Sector_Development_Program_Annual_Report-2024-EN.pdf
- SOCRadar – Saudi Arabia Threat Landscape Report 2024
  https://socradar.io/wp-content/uploads/2024/12/SOCRadar-Saudi-Arabia-Threat-Landscape-Report-2024.pdf
- SIRAR – Threat Landscape Report (Wide Analysis)
  https://www.sirar.com.sa/wp-content/uploads/2024/02/Threat-landscape-wide.pdf
- PwC – Global Digital Trust Insights 2025: Middle East Findings
  https://www.pwc.com/m1/en/publications/documents/2024/2025-global-digital-trust-insights-middle-east-findings.pdf
- SOCRadar – Middle East & Africa (MEA) Threat Report 2025
  https://socradar.io/wp-content/uploads/2025/10/MEA-Threat-Report-2025.pdf
- CS4CA – MENA Annual Cybersecurity Report 2025
  https://mena.cs4ca.com/wp-content/uploads/CS4CA-MENA-2025-Annual-Report.pdf
- TEM Journal – Cybersecurity Threats and Trends Study (2025)
  https://www.temjournal.com/content/142/TEMJournalMay2025_1791_1807.pdf