WHITEPAPER

Mapping Segura® Solutions to the Essential Cybersecurity Controls (ECC) of the National Cybersecurity Authority (NCA)

segura | Futureproof Identity Security | segura.security

Introduction

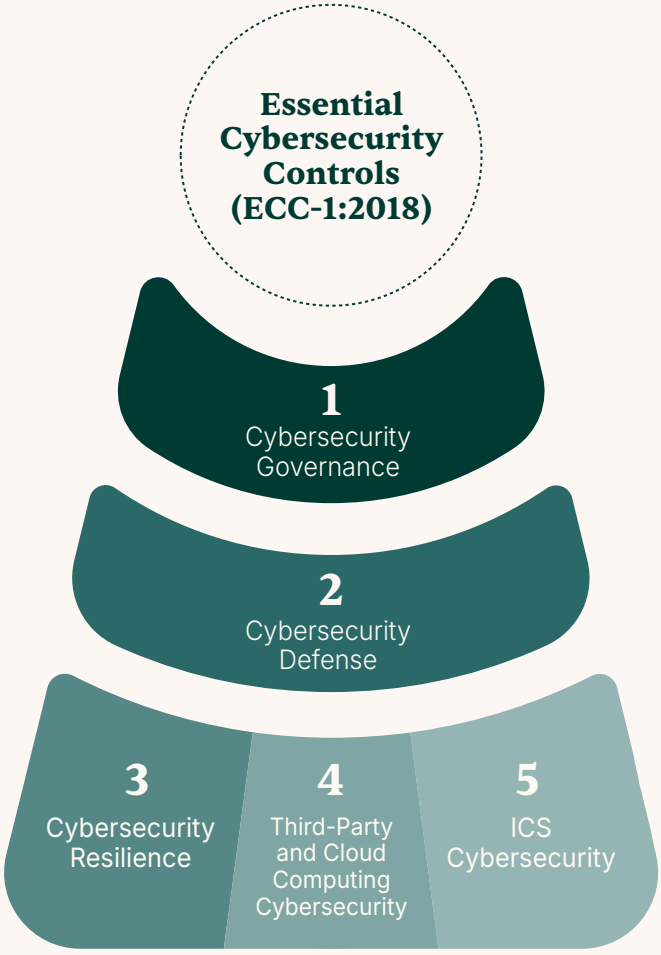
Cyberattacks targeting critical infrastructure are rising—globally and within the Kingdom. In response, Saudi Arabia established the National Cybersecurity Authority (NCA) and introduced the Essential Cybersecurity Controls (ECC-1:2018) to safeguard national interests and support Vision 2030.

These mandatory controls are now the foundation for cybersecurity compliance across government entities and Critical National Infrastructure (CNI) operators.

> This whitepaper shows how you can quickly align with ECC requirements using the Segura® 360° Privilege Platform—streamlining privileged access, remote connections, endpoint control, and secrets management. If you're looking for faster audit readiness, reduced risk, and full visibility, start here.

Understanding the ECC Framework

The Essential Cybersecurity Controls (ECC) were developed by Saudi Arabia's National Cybersecurity Authority (NCA) to establish a unified set of cybersecurity requirements across the public and private sectors.



ECC framework composition

Based on international best practices and aligned with the Kingdom's priorities, the ECC framework is designed to protect national infrastructure and critical information assets from modern cyber threats.

The ECC framework is composed of:

- **5 Main Domains**
- **29 Sub Domains**
- **114 Controls**

These controls apply to all government bodies and organizations managing CNI. They also offer valuable guidance for any entity working to improve its security maturity and compliance posture.

How Segura® Supports ECC Compliance

PAM Core

Segura® PAM Core delivers centralized, automated control of privileged accounts and credentials, enabling strong policy enforcement and regulatory compliance.

Key benefits include:

- Secure vaulting and automated password rotation
- Monitoring and recording of privileged sessions
- Just-in-Time access and least privilege enforcement
- Protection from credential misuse

PAM Core supports ECC controls focused on access governance, privileged session monitoring, and risk reduction, strengthening defenses against internal and external threats.

Endpoint Privilege Manager

Segura® Endpoint Privilege Manager extends access controls to user workstations and servers, reducing the attack surface and ensuring secure execution of applications.

Key benefits include:

- Local privilege management and application control
- Session logging for Windows and Linux endpoints
- Automatic credential injection without exposing passwords
- Enforcement of least privilege at the endpoint level

This solution supports ECC controls related to endpoint security, identity and access management, and malware prevention, helping organizations protect against lateral movement and privilege escalation.

Domum Remote Access

Segura® Domum provides secure, VPN-free remote access through a Zero Trust model—enabling controlled, monitored access for internal and third-party users.

Key benefits include:

- Agentless, browser-based access without VPN
- Full session monitoring and recording
- Granular access controls and time-limited permissions
- Seamless user experience for internal and external users

Domum aligns with ECC controls covering third-party cybersecurity, remote access governance, and session oversight to improve operational security and compliance.

DevOps Secrets Manager

Segura® DevOps Secrets Manager secures machine identities and secrets used across pipelines, enabling secure DevOps practices without slowing down delivery.

Key benefits include:

- Centralized vault for managing secrets across pipelines
- Integration with Jenkins, GitLab, Kubernetes, and other key tools
- Automated rotation and restricted credential access
- Monitoring and auditing of machine identity usage

This solution supports ECC requirements for identity and access management, cryptographic key protection, and secure automation in cloud-native and CI/CD environments.

ECC Compliance Mapping: Segura® Solutions

The table below outlines how each Segura® solution—PAM Core, Endpoint Privilege Manager, DevOps Secrets Manager, and Domum Remote Access—maps directly to ECC-1:2018 controls across key cybersecurity domains:

- Identity and Access Management
- Privileged Access and Session Control
- Remote Access Governance
- Endpoint and Network Security
- Secrets and Key Management
- Logging and Audit Readiness

By adopting Segura® solutions, organizations can streamline ECC implementation, improve visibility, and take control of cybersecurity risks across critical environments.

Subdomain: Periodical Cybersecurity Review and Audit

Periodical Cybersecurity Review and Audit

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 1-8-1 Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance with the cybersecurity controls in the organization.	✓	✓	✓	✓
ECC 1-8-2 Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function (e.g., Internal Audit function) to assess the compliance with the cybersecurity controls in the organization. Audits and reviews must be conducted independently, while ensuring that this does not result in a conflict of interest, as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.	✓	✓	✓	✓

Subdomain: Cybersecurity in Human Resources

To ensure that cybersecurity risks and requirements related to personnel (employees andcontractors) are managed fficiently prior to employment, during employment and aftertermination /separation as per organizational policies and procedures, and related laws and regulations.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 1-9-5 Personnel access to information and technology assets must be reviewed and removed immediately upon termination/ separation.	✓	✓		✓

Subdomain: Identity and Access Management

To ensure that the organization has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 2-2-1 Cybersecurity requirements for identity and access management must be defined, documentedand approved.	✓	✓	✓	
ECC 2-2-2 The cybersecurity requirements for identity and access management must be implemented.	✓	✓	✓	
The cybersecurity requirements for identity and access management must include at least the following: ECC 2-2-3-1 User authentication based on username and password.	✓	✓	✓	
ECC 2-2-3-2 Multi-factor authentication for remote access.		✓		
ECC 2-2-3-3 User authorization based on identity and access control principles: Need-to-Knowan d Need-to-Use, Least Privilege and Segregation of Duties.			✓	
ECC 2-2-3-4 Privileged access management.	✓	✓		
ECC 2-2-3-5 Periodic review of users' identities and access rights.	✓	✓	✓	

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 2-2-3-5 Periodic review of users' identities and access rights.	✓	✓	✓	
ECC 2-2-4 The Implementation of the cybersecurity requirements for identity and access management mustbe reviewed periodically.	✓	✓	✓	

Subdomain: Network Security Management

To ensure the protection of organization's network from cyber risks.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 2-5-3-1 Logical or physical segregation and segmentation of network segments usingfirewalls and defense-in-depth principles.		✓		
ECC 2-5-3-2 Network segregation between production, test and development environments.		✓		
ECC 2-5-3-5 Management and restrictions on network services, protocols and ports.		✓		

Subdomain: Cryptography

To ensure the proper and efficient use of cryptography to protect information assets as perorganizational policies and procedures, and related laws and regulations.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 2-8-3-2 Secure management of cryptographic keys during their lifecycles.	✓			✓

Subdomain: Cybersecurity Event Logs and Monitoring Management

To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization's operations.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 2-12-3-2 Activation of cybersecurity event logs on critical information assets.	✓	✓	✓	✓

Subdomain: Third-Party Cybersecurity

To ensure the protection of assets against the cybersecurity risks related to third-parties including out sourcing and managed services as per organizational policies and procedures, and related lawsand regulations.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 4-1-2-3 Requirements for third-parties to comply with related organizational policies and procedures, laws and regulations.		✓		

Subdomain: Industrial Control Systems (ICS) Protection

To ensure the appropriate and effective cybersecurity management of Industrial Controls Systems and Operational Technology (ICS/OT) to protect the confidentiality, integrity and availability of theorganization's assets against cyber attacks (e.g., unauthorized access, destruction, spying andfraud) in line with the organization's cybersecurity strategy and related and applicable local and international laws and regulations.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
ECC 5-1-3 In addition to the applicable ECC controls from the main domains (1), (2), (3) and (4), the cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) mustinclude at least the following: 5-1-3-1 Strict physical and virtual segmentation when connecting industrial productionnet works to othernetworks within the organization (e.g., corporate network).		✓		

Conclusion

The Essential Cybersecurity Controls (ECC) framework plays a vital role in strengthening cybersecurity across the Kingdom. But achieving compliance requires more than good intentions. It requires the right tools.

The Segura® **360° Privilege Platform** equips organizations with automation, traceability, and control to meet ECC standards with confidence.

By adopting **PAM Core, Endpoint Privilege Manager, DevOps Secrets Manager, and Domum Remote Access**, organizations can reduce risk, enforce least privilege, and ensure full traceability of sensitive actions—supporting both regulatory and operational goals.

About Segura®

Segura® (formerly senhasegura) is a cybersecurity company focused on Privileged Access Management (PAM). Its platform helps organizations secure and manage privileged identities, credentials, and secrets across hybrid and cloud environments.

Segura supports use cases such as credential vaulting, session monitoring, privilege elevation, and secrets management for DevOps. Designed to simplify complex identity security challenges, Segura provides IT teams with visibility, control, and tools to reduce risk and support compliance.

The company operates globally through a network of partners and serves customers across key sectors including finance, healthcare, government, telecom, and critical infrastructure.

WHITEPAPER

Mapping Segura® Solutions to the Essential Cybersecurity Controls (ECC) of the National Cybersecurity Authority (NCA)

Powered by MT4 Group | May 2025

segura® | Futureproof Identity Security | segura.security