Trellix

SOLUTION BRIEF

National Cybersecurity Authority (NCA) Cybersecurity Controls of Saudi Arabia

Leverage Trellix® to cybersecurity resilience and compliance

Trellix, a cybersecurity leader, aligns deeply with Saudi Arabia's vision for robust national cybersecurity. Trellix has been operating in the Kingdom of Saudi Arabia for the last two decades protecting some of the key organisations across every sector in the Kingdom when it comes to endpoint security, network security, and data security through its comprehensive GenAI-powered security Platform. As a trusted partner, Trellix supports the Kingdom's evolving digital transformation by ensuring that enterprises and government entities have access to cutting-edge solutions.

The **National Cybersecurity Authority (NCA)** in Saudi Arabia plays a pivotal role in safeguarding the Kingdom's critical infrastructure, businesses, and citizens from the growing threat of cyberattacks. As the central authority for cybersecurity in Saudi Arabia, the NCA establishes frameworks, policies, and guidelines to enhance the security posture of public and private entities. Trellix reinforces its commitment by enabling compliance with NCA standards and ensuring resilience against ever-evolving cyber threats.

This document maps the Trellix portfolio to all the three NCA controls ECC, CSCC & DCC for reference to organisations in Saudi Arabia.

What are Saudi NCA ECC, CSCC, and DCC?

Saudi Arabia's NCA established three cybersecurity control frameworks to strengthen the nation's digital infrastructure:

NCA ECC (Essential Cybersecurity Controls): A baseline framework designed to enhance the security of organizations by implementing fundamental cybersecurity measures, such as asset management, access control, and incident response.

NCA CSCC (Critical Systems Cybersecurity Controls): Aimed at safeguarding critical systems essential for delivering vital services. These controls focus on risk management, access security, and the protection of critical information infrastructure.

NCA DCC (Data Cybersecurity Controls): Focused on ensuring the protection of sensitive data throughout its lifecycle, including classification, encryption, and access control, aligned with organizational and legal requirements.

Who is Affected by NCA ECC, CSCC, and DCC?

The NCA frameworks apply to a broad range of organizations across Saudi Arabia, including:

- Government Entities: Sectors that manage sensitive data and critical services.
- Critical Infrastructure Providers: Energy, transportation, and healthcare sectors.
- Private Sector Organizations: Industries such as telecommunications, banking, and manufacturing, especially those handling sensitive data or essential services.
- Digital Service Providers: Cloud, software, and IT services offerings.

Compliance is essential for ensuring the safety, reliability, and resilience of the Kingdom's digital ecosystem.

Why Use Trellix for Saudi NCA ECC, CSCC, and DCC?

Trellix provides an extensive suite of cybersecurity solutions and services that align with the NCA ECC, CSCC, and DCC frameworks while adhering to international standards such as NIST Cybersecurity Framework, ISO27001.

Comprehensive Coverage: Trellix solutions and services address critical areas, including endpoint security, network protection, and data security.

Integrated Approach: Tools like Trellix ePolicy Orchestrator (ePO) provide centralized management, ensuring streamlined compliance efforts.

Advanced Threat Intelligence: Leveraging Trellix insights and detection capabilities, organizations can stay ahead of emerging threats.

Trellix Solutions Aligned with NCA ECC, CSCC, and DCC

Category	Product	Description	NCA Controls
Endpoint Security	Trellix Endpoint Security	Provides multi-layered protection in a single agent for devices across on-premises, cloud, and disconnected environments, managed through a single console.	ECC: 2-3-3 CSCC:2-3-1-1 & 2-3-1-2
	Trellix Endpoint Detection and Response (EDR)	Offers proactive detection and response capabilities to identify and contain threats swiftly.	CSCC: 2-11-1-3
	Trellix Application and Change Control	Ensures only authorized applications run on devices, reducing the risk of malicious software execution.	CSCC: 1-3-2-1 & 2-3-1-8 & 2-3-1-1
	Trellix Mobile Security	Secures mobile devices against threats, ensuring data protection and compliance.	ECC: 2-6-3 DCC 2-3-1-1 & 2-3-1-2 & 2-3-1-3

Category	Product	Description	NCA Controls
Endpoint Security	Trellix Device Control	Comprehensive device management helps control and block confidential data copied to removable storage devices, including over Bluetooth.	ECC: 2-3-3-2
	Trellix Policy Auditor	Automate and simplify compliance, patch, and security configuration audits across enterprise environments.	ECC: 2-3-3-3 CSCC: 1-2-1-1 & 2-2-1-1 & 1-4-1 & 2-3-1-6 DCC: 2-2-1-1
	Trellix ePolicy Orchestrator (ePO)	Automate and simplify compliance, patch, and security configuration audits across enterprise environments.	CSCC: 2-1-1-1
	Compromise Assessment Service	Pinpoint active threats within your environment to identify malware and remote command and control from information collected from the endpoints. This is matched against the behavior of your endpoints with Trellix custom cyber intelligence content and processing system.	ECC: 2-3-3 & 2-3-3-3 CSCC:2-3-1-1 & 2-3-1-2 & 1-3-2-1 & 2-3-1-8 & 2-11-1-3 & 1-2-1-1 & 2-2-1-1 & 1-4-1 & 2-3-1-6 DCC: 2-2-1-1
Network Security	Trellix Network Security	Detects and blocks advanced threats, lateral movement, and suspicious network behavior in real time.	ECC: 2-5-3-8 CSCC: 2-4-1-5
	Trellix Network Forensics	Identify and resolve a broad range of security incidents faster with lossless network data capture and retrieval with centralized analysis and visualizations.	
	Trellix Intrusion Prevention System	Inspect all network traffic to prevent new and unknown attacks with advanced detection and emulation techniques with a high degree of accuracy and performance.	ECC: 2-5-3-6 & 2-5-3-9
	Incident Response and Forensics Service	Assist in dealing with network and/or computer security incidents such as computer intrusions, large scale virus outbreaks, and other unacceptable events that threaten an organization's effectiveness, reputation, and its more tangible assets.	ECC: 2-5-3-8 & 2-5-3-6 & 2-5-3-9 CSCC: 2-4-1-5
Email Security	Trellix Email Security	Safeguards email communications from phishing, malware, and other threats.	ECC: 2-4-3-1 & 2-4-3-4
	Trellix IVX for Enterprise Applications	Provides comprehensive protection across various enterprise communication channels.	ECC:2-4-3-1 & 2-4-3-4 & 2.4.3.5
	Ransomware Resilience Assessment (RRA) Service	Leverages the anatomy of ransomware to assess existing controls to identify gaps and capabilities to handle a ransomware incident.	ECC: 2-4-3-1 & 2-4-3-4 & 2.4.3.5
Data Security	Trellix Data Loss Prevention Endpoint Complete	Prevents unauthorized data transfers and leaks across various channels.	CSCC: 2-6-1& DCC: 2-4-1-1 & 2-4-1-2
	Trellix Data Loss Prevention Network Prevent	Prevent users from sharing unauthorized information across networks.	ECC: 2.5.3.3

Category	Product	Description	NCA Controls
Data Security	Trellix Data Encryption	Ensures sensitive data is encrypted both at rest and in transit.	ECC: 2-8-3 CSCC: 2-7-1 DCC: 2-5-1
	Trellix Database Security	Monitors and protects databases from threats and unauthorized access.	ECC: 2-10-3 CSCC: 2-2-1-8 & 2-9-1-1
	Data Security Assessment and Data Protection Program Development Service	Start with a Data Protection Workshop to come up with a cross-functional, global definition of your known critical data and understand the data security and protection regulatory requirements. Then build a data governance program encompassing the overall management of the confidentiality, integrity and availability of data with defined data classification levels and sound policies, standards, and procedures that are fundamental to an effective DLP strategy.	CSCC: 2-6-1 & 2-7-1 & 2-2-1-8 & 2-9-1-1 DCC: 2-4-1-1 & 2-4-1-2 & 2-5-1 ECC: 2.5.3.3 &: 2-8-3 & 2-10-3
SOC-SIEM	Trellix Enterprise Security Manager	Conduct streamlined, efficient security information and event management from a holistic foundation.	ECC: 2-12 CSCC: 2-11
	Red Teaming Service	Red Teaming exercises combine elements of social engineering with penetration testing to gain insight into how the environment will fair in a real-world attack scenario. Attack scenarios can be crafted to emulate specific types of threat actors (enthusiasts, organized groups, and cyber-criminals) employing both traditional and non-traditional techniques to test your resilience against intrusions, data exfiltration, fraud, internal attack, corporate espionage, physical compromise, etc.	ECC: 2-12 CSCC: 2-11
Threat Intelligence	Trellix Threat Intelligence Exchange	Transform security infrastructure into a collaborative system	ECC: 2.13.3.5
	Threat Intelligence Maturity Assessment and Practice Development Service	Identify key stakeholders and role players, then conduct interviews with said stakeholders and role players to understand the current maturity of your CTI program, business vertical CTI influences, and relevant core principles. Then, build your Threat Intelligence Practice to enhance your view of the threat landscape, enabling effective protection, detection, and response.	ECC: 2.13.3.5
File Protection	Trellix File Protect (FX)	Detects and eliminates malware residing in network file shares and content repositories, preventing the lateral spread of threats within an organization.	ECC: 2-3-3-1 CSCC: 2-3-1-2
	Cybersecurity Controls Configuration review Service	Review and manually validate control security configuration settings on each system and ensure that they are consistent with industry standard best practice, security guidelines and recommendations.	ECC: 2-3-3-1 CSCC: 2-3-1-2

Category	Product	Description	NCA Controls
Skyhigh Security	Proxy	Monitor and control access to sensitive information.	ECC: 2-5-3-3
	Web Applications, Mobile Applications and API Security Assessment Service	Employ a comprehensive methodology during web applications, Mobile applications, and API Security assessments encompassing test scenarios ranging from zero-knowledge "black box" to full-access "white box" testing. This will cover an iterative approach of several assessment models such as quick scan, complete assessment, OWASP top ten, and gray box model that cater to your business needs, along with Trellix's proprietary process consisting of over 100 checks.	ECC: 2-5-3-3
	Cloud Configuration Review Service	egin with network level scans to verify that the underlying infrastructure is configured appropriately and is free of security issues. These scans target the server's operating system and web server software. Next, follow up with manual checks to verify the results of the scan and attempt to identify additional issues. Subsequently, move to a manual configuration review of all cloud services that reside in your infrastructure.	ECC: 2-5-3-3

The three frameworks form a comprehensive strategy to strengthen Saudi Arabia's cybersecurity ecosystem and enable entities to align with the Kingdom's Vision 2030 digital transformation objectives.

Through tailored solutions and strategic partnerships, Trellix is dedicated to securing Saudi Arabia's digital economy and fostering a safer cyberspace, contributing to the Kingdom's ambitious Vision 2030.

For more information please refer to www.trellix.com.