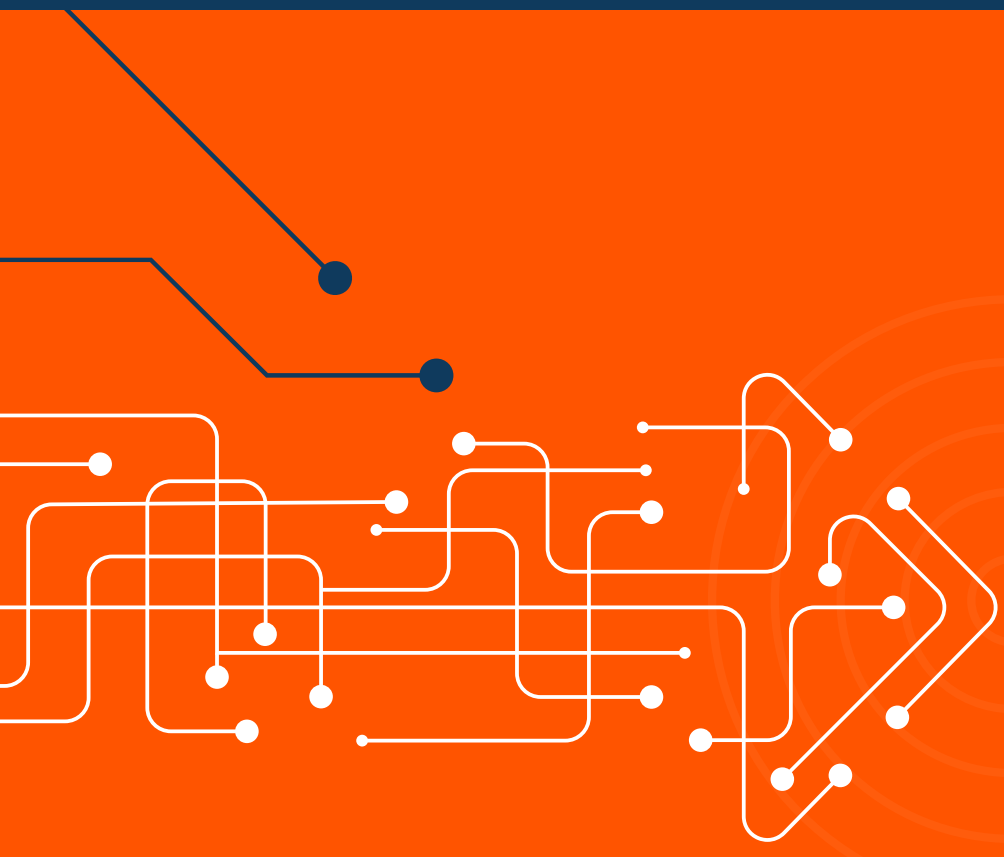
BeyondTrust

Mapping BeyondTrust Capabilities to KSA's NCA Essential Cybersecurity Controls



This document is informational and is intended to provide guidance on how organizations may use BeyondTrust products to meet their own obligations under The Kingdom of Saudi Arabia's NCA ECC. BeyondTrust is not representing that we are subject to or compliant with NCA ECC.

BeyondTrust

TABLE OF CONTENTS

Overview

The Kingdom of Saudi Arabia's Vision 2030 aims for a comprehensive improvement of the nation and its security, economy, and citizens' well-being. Naturally, one of the essential goals of Vision 2030 is the transformation towards digitalization and the improvement of digital infrastructure. Vision 2030 aims to keep up with the global acceleration in digital services, renewable global networks, IT systems, and OT systems, align with growing computer processing and massive data storage and exchange capabilities, and prepare for an explosion in artificial intelligence growth and the transformations that come with a fourth industrial revolution.

This guide has been prepared so that IT and security administrators can quickly understand how BeyondTrust Identity Security and Privileged Access Management (PAM) solutions map to requirements set by the Kingdom of Saudi Arabia's National Cybersecurity Authority (NCA) Essential Cybersecurity Controls (ECC).

The National Cybersecurity Authority (referred to in this document as "The Authority" or "NCA") developed the Essential Cybersecurity Controls (ECC) after conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards. This research involved studying related national decisions, laws, and regulatory requirements, reviewing and leveraging cybersecurity best practices, analyzing previous cybersecurity incidents and attacks on government and other critical organizations, and surveying and considering opinions of multiple national organizations.

The Essential Cybersecurity Controls consist of the following:

- 4 Cybersecurity Main Domains
- 28 Cybersecurity Subdomains
- 108 Cybersecurity Main Controls
- 92 Cybersecurity Sub Controls

This document is based on the original Essential Cybersecurity Controls (ECC–1:2018), updated to include changes in ECC – 2: 2024.

What Is the Policy Objective?

The main objective of these controls is to set the minimum cybersecurity requirements for information and technology assets in organizations. These requirements are based on industry leading practices which will help organizations minimize the cybersecurity risks that originate from internal and external threats.

Organizations should focus on the following key objectives to protect information and technology assets:

- Confidentiality
- Integrity
- Availability

These controls take into consideration the following four main cybersecurity pillars:

- Strategy
- People
- Processes
- Technology

Who Needs to Implement the National Information Assurance Policy?

Compliance with these standards will raise the level of information assurance within the Kingdom of Saudi Arabia and help the Kingdom progress towards a more resilient national information and communication infrastructure, and cyberspace.

These controls are applicable to government organizations in the Kingdom of Saudi Arabia (including ministries, authorities, establishments, and others) and their companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs), which are all referred to herein as "The Organization." The NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their cybersecurity.

These controls have been developed after taking into consideration the cybersecurity needs of all organizations and sectors in the Kingdom of Saudi Arabia. Every organization must comply with all applicable controls in this document.

To comply with item 3 of article 10 of NCA's mandate (and as per the Royal Decree number 57231 dated 10/11/1439H), all organizations within the scope of these controls must implement whatever necessary to ensure continuous compliance with the controls.

NCA evaluates organizations' compliance with the ECC through multiple means, such as self-assessments by the organizations, periodic reports of the compliance tool, or on-site audits.

Assessment and Compliance Tool
The NCA will issue a tool (ECC-2:2024 Assessment and Compliance Tool) to organize the process of assessment and measurement of compliance by entities in applying the ECC.

ECC Domains and Structure

The following graphic shows the main domains of the ECC:

National Cybersecurity Authority - Essential Cybersecurity Controls (ECC-1: 2024), Main domains of ECC, p.10

1. Cybersecurity Governance	1-1	Cybersecurity Strategy	1-2	Cybersecurity Management
	1-3	Cybersecurity Policies and Procedures	1-4	Cybersecurity Roles and Responsibilities
	1-5	Cybersecurity Risk Management	1-6	Cybersecurity in Information and Technology Project Management
	1-7	Compliance with Cybersecurity Standards, Laws and Regulations	1-8	Periodical Cybersecurity Review and Audit
	1-9	Cybersecurity in Human Resources	1-10	Cybersecurity Awareness and Training Program
2- Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	Information Systems and Information Processing Facilities Protection	2-4	Email Protection
	2-5	Network Security Management	2-6	Mobile Devices Security
	2-7	Data and Information Protection	2-8	Cryptography
	2-9	Backup and Recovery Management	2-10	Vulnerability Management
	2-11	Penetration Testing	2-12	Cybersecurity Event Logs and Monitoring Management
	2-13	Cybersecurity Incident and Threat Management	2-14	Physical Security
	2-15	Web Application Security		
3- Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4- Third-Party and Cloud Computing Cybersecurity	4-1	Third-Party Cybersecurity	4-2	Cloud Computing and Hosting Cybersecurity

How BeyondTrust Solutions Can Help

BeyondTrust capabilities address 19 individual controls across 4 of the 5 main domains within the **National Cyber Security Authority Essential Cybersecurity Controls.**

This mapping guide explains how you can use BeyondTrust solutions to map to the NCA ECC to maintain security and more easily demonstrate and maintain compliance.

Each **NCA ECC** policy requirement is outlined in the following sections and are mapped to these BeyondTrust solutions:

- **Identity Security Insights®** – Gives organizations unified visibility into identity risk by continuously analyzing human and non-human identities, privileges, and access paths—revealing hidden escalation risks and enabling proactive threat detection and remediation.
- **Entitle** - Cuts off privilege attack paths by eliminating always-on access, replacing it with just-in-time (JIT) automation that reduces risk--without slowing down teams.
- **Password Safe®** - Enables automated discovery, onboarding, management, and auditing of all privileged accounts, privileged credentials (passwords, secrets, keys, etc.).
- **Privileged Remote Access** - Delivers secure, just-in-time remote access to cloud, on-premises, and OT environments—using identity-based controls, credential injection, and session auditing—without requiring VPNs.
- **Endpoint Privilege Management** - Combines least privilege enforcement and application control to manage and reduce admin privileges across Windows, macOS, Unix, and Linux systems. The product ensures only approved applications and tasks may run with elevated permissions, while maintaining user productivity and security compliance.
- **Remote Support** – Enables service desk technicians to support any user or device, anywhere, all while ensuring enhanced security. Applies least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.
- **Active Directory Bridge** - Extends Microsoft Active Directory authentication, SSO, and policy controls to Unix and Linux systems—enabling centralized identity management, consistent access enforcement, auditing, and compliance across mixed operating system environments.

The controls matrix on the following pages highlights the primary applicable NCA ECC requirements that your organization can address by leveraging the capabilities within BeyondTrust solutions. This is not meant to be an exhaustive list, but rather highlight the most relevant features for supporting alignment to the NCA ECC framework.

Controls Chart

Subdomain Name	Objetive	Control Ref. Number	Control Clauses	Identity Security Insights	Entitle	Endpoint Privilege Management	Privileged Remote Access	Password Safe	Remote Support	Active Directory Bridge
Identity and Access Management	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.	ECC 2-2-1	Cybersecurity requirements for identity and access management must be defined, documented, and approved.	✓	✓	✓	✓	✓		✓
		ECC 2-2-2	The cybersecurity requirements for identity and access management must be implemented.	✓	✓	✓	✓	✓		✓
		ECC 2-2-3	The cybersecurity requirements for identity and access management must include at least the following:							
			2-2-3-1 Single-factor authentication based on username and password.	✓	✓	✓	✓	✓		
			2-2-3-2 Multi-factor authentication, and defining the suitable authentication factors and their numbers as well as the suitable authentication techniques based on the result of impact assessment of authentication failure and bypass for remote access and for privileged accounts.	✓	✓	✓	✓	✓		✓
			2-2-3-3 User authorization based on identity and access control principles: Need-to-Know and Need-to-Use, Least Privilege and Segregation of Duties.	✓	✓	✓	✓	✓		✓
			2-2-3-4 Privileged access management.	✓	✓	✓	✓	✓		✓
			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 must be reviewed periodically.			✓	✓	✓	✓	✓

Networks Security Management	To ensure the protection of organization's network from cyber risks.	ECC 2-5-3	2-5-3-1 Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles.				✓		✓	
			2-5-3-2 Network segregation between production, test, and development environments.				✓		✓	
			2-5-3-5 Management and restrictions on network services, protocols, and ports.	✓			✓		✓	
Cryptography	To ensure the proper and efficient use of cryptography to protect information assets as per objective organizational policies and procedures, and related laws and regulations.	ECC 2-8-3	2-8-3-2 Secure management of cryptographic keys during their lifecycles.	✓				✓		
Vulnerabilities Management	To ensure timely detection and effective remediation of technical vulnerabilities to Objective prevent or minimize the probability of exploitation of these vulnerabilities by cyber-attacks and to reduce any impacts on the entity's business.	ECC 2-10-3	Cybersecurity requirements for technical vulnerabilities management within the entity shall be identified, documented, and approved.	✓	✓				✓	
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.	ECC 2-12-3	2-12-3-2 Activation of cybersecurity event logs on remote access and privileged user accounts.	✓	✓	✓	✓	✓	✓	✓
Periodical Cybersecurity Review and Audit	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.	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.	✓	✓	✓	✓	✓		✓

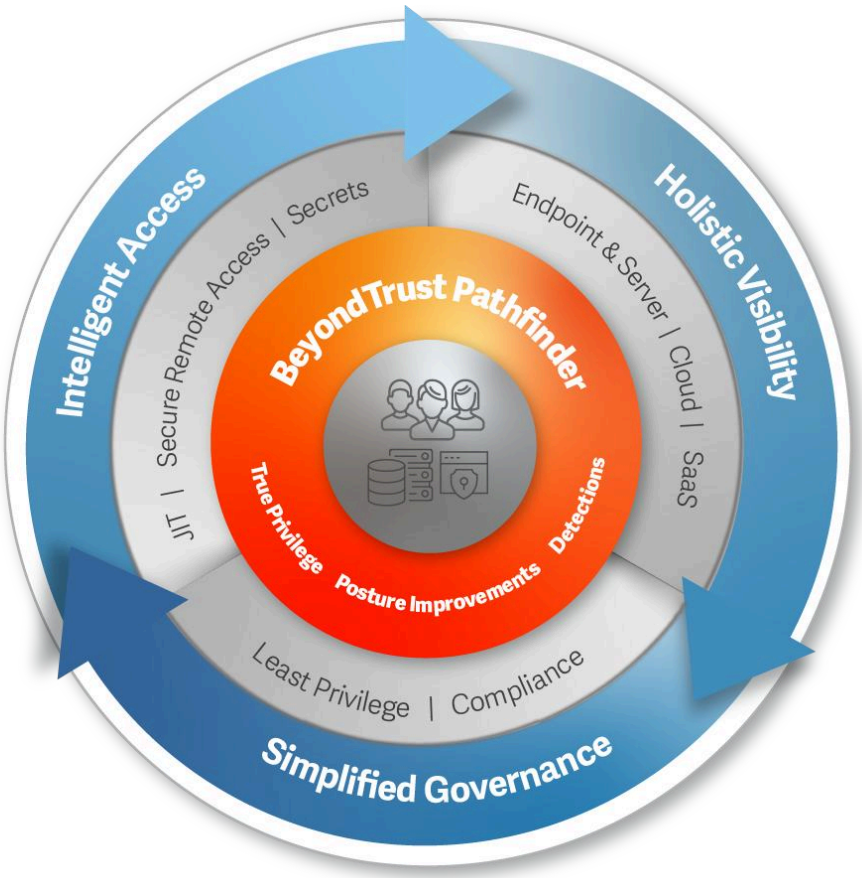
Periodical Cybersecurity Review and Audit	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.	ECC 1-8-2	Cybersecurity audits and reviews must be conducted by 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.			✓	✓	✓		✓
Cybersecurity in Human Resources	To ensure that cybersecurity risks and requirements related to personnel (employees and contractors) are managed efficiently prior to employment, during employment and after termination/ separation as per organizational policies and procedures, and related laws and regulations.	ECC 1-9-5	Personnel access to information and technology assets must be reviewed and removed immediately upon termination/ separation.		✓		✓	✓		✓
Third-Party Cybersecurity	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services as per organizational policies and procedures, and related laws and regulations.	ECC 4-1-2	4-1-2-3 Requirements for third parties to comply with related organizational policies and procedures, laws and regulations.	✓	✓		✓			
Cloud Computing and Hosting Cybersecurity	To ensure proper and efficient remediation of cyber risks and implementation of cybersecurity requirements for cloud computing and hosting, as per the entity's regulatory policies and procedures, relevant legislative and regulatory requirements, orders, and decisions, and to ensure the protection of the entity's information and technology assets on cloud computing services hosted, processed, or managed by third parties.	ECC 4-1-2	In accordance with the relevant legislative and regulatory requirements, and in addition to the applicable controls in the Main Domains (1), (2), and (3) and Subdomain (4.1) that are necessary to protect the entity's data or services provided thereto, cybersecurity requirements for use of cloud computing and hosting services shall include the following as a minimum:				✓	✓		
			4.2.3.2 Separation of the entity's environment (especially virtual servers) from environments of other entities within the cloud computing service provider.							

The BeyondTrust Pathfinder Platform

The BeyondTrust Pathfinder Platform unifies identity visibility, intelligence, and control into a single, AI-driven control plane. It maps and manages privilege relationships across human, machine, AI agent, and workload identities—revealing hidden Paths to Privilege™ and enabling proactive risk reduction across your entire identity attack surface.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. BeyondTrust was named a Leader in both the **The Forrester Wave™: Privileged Identity Management Solutions, Q3 2025 report** and the **Gartner® Magic Quadrant™ for Privileged Access Management.** We believe these accolades reflect strong execution and a comprehensive vision for identity security.

As a centrally managed, extensible platform, Pathfinder allows organizations to deploy a full set of PAM and identity security capabilities at once—or adopt them incrementally over time—while maintaining unified visibility, consistent policy enforcement, and operational efficiency from a single, unified console.



About BeyondTrust

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**