WHITEPAPER

Mapping BeyondTrust Capabilities to KSA's NCA ECC Controls

BeyondTrust

Table of Contents

Overview 3
What is the Policy Objective? 3
Controls Chart 6
The BeyondTrust Privileged Access Management Platform 9
About BeyondTrust 10

Overview

This guide has been prepared so that IT and security administrators can quickly understand how BeyondTrust Privileged Access Management (PAM) solutions map into requirements set forth in 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, studying related national decisions, law 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:

- 5 Cybersecurity Main Domains
- 29 Cybersecurity Subdomains
- 114 Cybersecurity Controls

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. The following key objectives must be focused on in order to protect the organization's 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 its 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.

ECC Domains and Structure

The following graphic show the main domains of the ECC:

National Cybersecurity Authority - Essential Cybersecurity Controls (ECC-1: 2018), Main domains of ECC, p.11

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 white paper explains how to map BeyondTrust solutions to the **NCA ECC** to maintain security and more easily demonstrate and maintain compliance. BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges.

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

- (PPM) Privilege Password Management- Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities.

- (SRA) Secure Remote Access - Apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.

- (EPM) Endpoint Privilege Management - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

- (DSS) Devops Secrets Safe - Secure and automate the storage and access of secrets used by applications, tools, and other processes across your development operations environments.

The tables on the following page highlights the primary applicable NCA ECC requirements that are addressed by capabilities within BeyondTrust solutions. This is not an exhaustive list but includes the most relevant features for supporting the NCA ECC framework.

Controls Chart

Subdomain name	Objective	Control Ref. Number	Control Clauses	BeyondTrust Product				
				PPM	SRA	EPM/ PMUL	ADB	DSS
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 User authentication based on username and password;	✓	✓	✓	✓	
			2-2-3-2 Multi-factor authentication for remote access;		✓			
			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.	✓				✓
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	ECC 1-8-1	Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance	✓	✓	✓	✓	

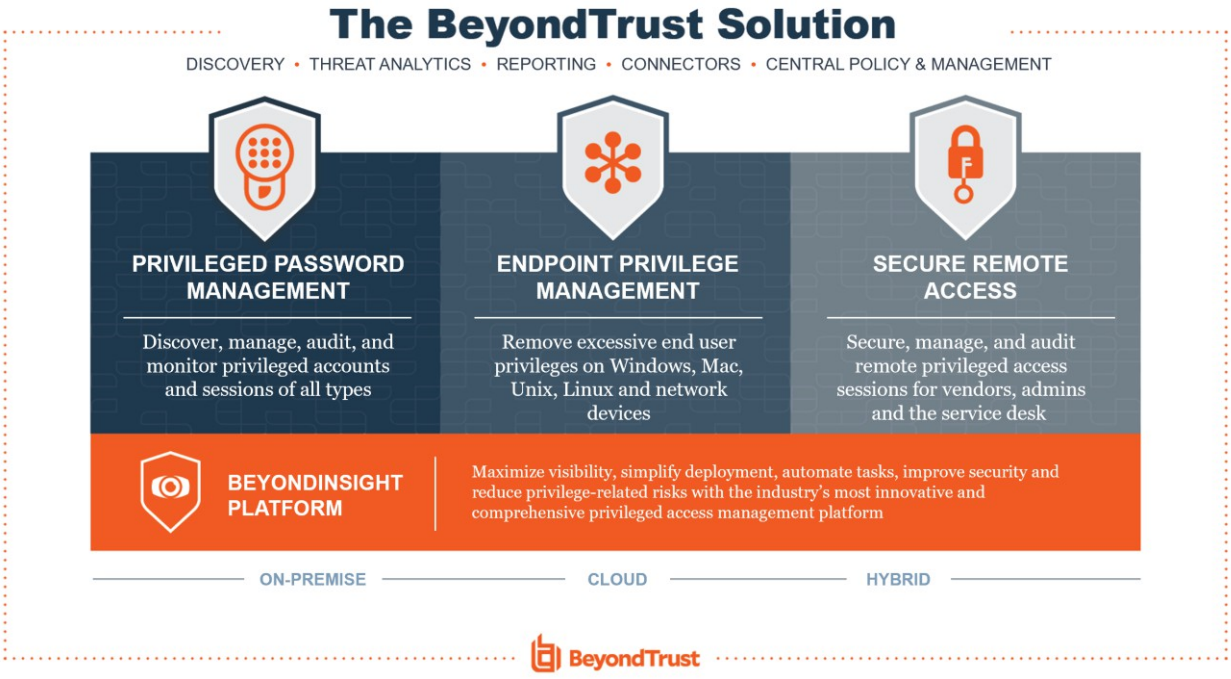
	organizational policies and procedures, as well as related national and international laws, regulations and agreements.		with the cybersecurity controls in the organization.					
		ECC 1-8-2	Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function (e.g., 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.	✓	✓	✓	✓	
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.		✓			
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 the organization's assets against cyber-attacks (e.g., unauthorized access, destruction, spying and fraud) in line with the organization's cybersecurity strategy and related and applicable local and international laws and regulations.	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) must include at least the following: 5-1-3-1 Strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network).		✓			

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Forrester Wave Privileged Identity Management, Q4 2020, BeyondTrust is named as a leader and ranked as the top Vendor in the strategy category.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.