BeyondTrust

This paper will examine some of the key aspects of the Cybersecurity Code of Practice for Critical Information Infrastructure.

Aligning to the Singapore Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure with BeyondTrust

Introduction

What is the CCoP?

First issued in 2018 and updated in 2022, the *Cybersecurity Code of Practice for Critical Information Infrastructure* (CCoP) specifies the minimum cybersecurity standards for operators of Critical Information Infrastructure (CII) in Singapore to implement in their organisations. The effective date for this regulation is 4th July 2022.

The CCoP is overseen by the Cyber Security Agency of Singapore (CSA), whose mission is to protect the cyber interests of Singaporean citizens and businesses, including protecting and defending Critical Information Infrastructure.

As the Code dictates, individual operators are "expected to implement measures beyond those stipulated in this Code to further strengthen the cybersecurity of the CII based on the cybersecurity risk profile of the CII." Given the ongoing and increasingly advanced threats to both Information Technology (IT) and Operational Technology (OT) environments, the CCoP outlines minimum cybersecurity requirements to ensure all entities operating under Singaporean purview are adequately protected.

This paper will examine some of the key aspects of the *Cybersecurity Code of Practice for Critical Information Infrastructure* and examine how Singaporean organisations under this regulation can meet requirements using Privileged Access Management (PAM) solutions, including those from BeyondTrust.

It is recommended that any operators of CII (CIIOs) review the full documentation on the CSA website.

The Role of Privileged Access Management

Like many similar regulations around the world, much of what is required by the CCoP is based on existing cybersecurity standards, models, and demonstrated best practices, including concepts like zero trust. Privileged Access Management capabilities are frequently relied on by organisations complying with global cybersecurity requirements and regulations.

Core Privileged Access Management capabilities include:

- Enforcement of least privilege, restricting access rights and permissions.
- Visibility, control, and auditing of privileged identities and sessions.
- Secure management of privileged credentials across human and machine identities.

As global businesses, governments, and institutions grapple with heightened cyber threats – and the potential damages they may cause – PAM provides a significant amount of defense against privilege abuse, lateral movement, and credential compromise.

Cybersecurity Design Principles in the CCoP

"Cybersecurity design principles underpin the security architecture of the system and network. Adopting these principles and taking proactive steps to integrate security into the design process helps to reduce the overall attack surface of the system and network by various means. Often, this can discourage a cyber-attack as it would significantly increase the time and effort required by a cyber threat actor to compromise the system and network."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 3.5

Section 3 of the *Cybersecurity Code of Practice for Critical Information Infrastructure* establishes the frameworks to ensure that the cybersecurity strategies are aligned with business objectives, as well as providing guidance on how to evaluate, define, and direct efforts towards managing cybersecurity risks. While most of this section discusses organisational and policy frameworks, Section 3.5 introduces Cybersecurity Design Principles – a collection of principles which should be adopted by Singaporean organisations to reduce cyber risks among people, processes, and technologies.

Many of the design principles and proactive steps requested within the CCoP are directly provided by Privileged Access Management solutions, including BeyondTrust PAM. The following Cybersecurity Design Principles are excerpted from the official document to illustrate how BeyondTrust PAM can help those Singaporean institutions subject to the CCoP meet key requirements.

Defence in Depth (3.5.1 a)

"The defence-in-depth principle to ensure that the security architecture of the CII includes multiple layers of security controls to prevent single point of failure;"

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 3.5.1 a

No single security practice can provide complete coverage against cyber threats. As cybersecurity protocols grow in complexity and scale, attacks have consequently evolved to target multiple points along the chain. Alternatively, many attack methods employ several steps themselves.

For example, privilege escalation attacks typically involve multiple steps starting with account hijacking. There are multiple steps in the attack kill chain where the threat might be stopped by leveraging technologies including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Privilege Access Management (PAM), and network segmentation.

BeyondTrust's Privileged Access Management platform establishes a powerful, blended defense against cyberattack, minimising points of failure along the cyber kill chain, and substantially shrinking the threat surface. By eliminating excess privileges, locking down remote access pathways, and securing privileged credentials, BeyondTrust's PAM platform creates an environment inhospitable to cyberattacks and prevents potential attacks from moving laterally across systems.

The Principle of Least Privilege (3.5.1 b)

"The least privilege principle to ensure that accounts and users are granted the least extent of access necessary to perform their required functions;"

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 3.5.1 b

As a component of the concept of zero trust, least privilege is a long-held cybersecurity principle which dictates that users should only have access to the resources and privileges that they need to do their job for the time necessary to complete the task – and nothing more.

In practice, least privilege can substantially reduce the window for successful attacks. Excessive privileges or access that would be exploited for malicious purposes, either by employees or external threat actors, are limited or eliminated until absolutely needed.

BeyondTrust's PAM platform provides numerous ways to support the implementation of least privilege, including:

- Implementing just-in-time privileges, where privileges are only elevated for the application or applications needed and only for the necessary length of time to complete the task.
- Removing admin rights on all endpoints and root and admin accounts on servers.
- Auditing and managing all privileged accounts, including all user and local accounts, SSH keys, Windows and Linux groups, and DevOps secrets.
- Managing the rotation of passwords for privileged accounts, including one-time passwords.

Principle of Segregation of Duties (3.5.1 c)

"The principle of segregation of duties to ensure that duties and responsibilities for critical functions relating to the CII are divided among different persons."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 3.5.1 c

This principle is designed to put layers or "moats" between various critical accounts and capabilities related to Critical Information Infrastructure. Complementing the principle of least privilege, the segregation of duties limits the ability of threat actors to access privileged accounts and to contain their movement closer to the point of entry should they gain access to credentials

For example, an account with admin privileges that opens a malicious file or email would very quickly provide the attacker with the same privileges.

To provide an important layer of privilege separation, PAM solutions support role-based access while separating administrative account functions from standard account requirements. Privileged Access Management also separates auditing and logging capabilities within the administrative accounts themselves.

Zero Trust (3.5.2 b)

"The zero-trust principle to ensure that each request for access to the CII is authenticated, authorised and validated for security configuration and posture before access is granted."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 3.5.2 b

Described by the United States' National Institute of Standards and Technology (NIST) as a paradigm, **Zero Trust** embodies the practice of "never trust, always verify." Highly relevant in a modern business landscape of distributed employees and resources, zero trust requires the continual verification that users are who they say they are – and enforces protocols for distributing privileges and access accordingly.

As mentioned previously, the principle of least privilege is fundamental to zero trust and therefore foundational in meeting the requirements of the CCoP. The central value that organisations derive from PAM solutions includes enabling and enforcing least privilege, continuous authentication and auditing of privileged users and their activity, including both employees and third parties, and the operationalisation of zero trust principles.

The BeyondTrust PAM platform is no exception. BeyondTrust Privileged Access Management solutions help enable NIST's seven core tenets of zero trust by working relentlessly to identify and secure every privileged user (human, non-human, employee, vendor), asset, and session across the digital estate.

This includes capabilities that:

- Enforce adaptive, least privilege control for all access.
- Isolate, monitor, manage, and audit privileged sessions.
- Prevent lateral movement and privilege escalation attacks.

Third-Party Access (3.8.1, 3.8.2)

"3.8.1: The CIIO shall remain responsible and accountable for the cybersecurity of the CII even if it engages an external party to perform or assist in performing any functions, activities or operations in respect of the CII (referred to below as "outsourcing").

3.8.2: The CIIO shall establish processes to maintain oversight over all outsourced functions, activities or operations, in order to minimise cybersecurity exposure arising from such outsourcing."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Sections 3.8.1 & 3.8.2

The governance requirements within the CCoP includes Section 3.8, Outsourcing and Vendor Management. This section specifically notes that Critical Information Infrastructure operators must ensure that there are cybersecurity controls in place to mitigate the risks around third parties interacting with CII systems.

In recent years, much more of the work conducted by outsourcers and third-party suppliers has been done remotely. Typically, this work has been accomplished by leveraging technologies such as VPNs – technologies that often provide wide privileged access with limited oversight into the actions of the user. A shocking number of high-profile data breaches and cyberattacks have been directly linked back to examples of this kind of remote access.

BeyondTrust's solutions provide a secure alternative to VPNs. BeyondTrust solutions are designed to implement the principle of least privilege, ensuring users have access to the resources required to carry out a task but nothing more – even including tasks as discreet as stopping or starting a service on a server. All of this is accomplished without ever having access to their credentials. A full audit of the actions of the user is available and users can be promptly onboarded and offboarded, with the beginning and ending of projects.

CCoP Protection Requirements

"Protection requirements help the CIIO understand and implement the required people, process, and technology controls to protect the CII and to limit and contain the impact of cybersecurity incidents."

- Cybersecurity Code of Practice for Critical Information Infrastructure

Section 5 of the Code outlines several specific protection requirements that Critical Information Infrastructure operators must put into place to prove compliance. In the next section of this whitepaper, we will examine these Protection Requirements requested by the CCoP for Singaporean organisations – and how solutions within the BeyondTrust PAM platform can meet them one-by-one.

Account Management (5.2)

"Asset owners should determine appropriate access rights for each specific account while taking into consideration the associated cybersecurity risks. Accounts should not be granted excessive and unnecessary privileges to prevent unauthorised access. In addition, processes need to be established to detect unauthorised activities."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 5.2

The importance of managing and reporting on privileged accounts is heavily emphasised in the Code within Sections 5.2 and 5.3, covering Account Management and Privileged Access Management, respectively.

The Account Management section (5.2) lists the capabilities and security controls that CIIOs must have in place around user, application, service, and system accounts. Namely, this section lists least privilege controls, removal of shared user accounts, activity and session monitoring, and removal of install or local admin rights as paramount requirements – all of which are core features of BeyondTrust **Privilege Management for Windows and Mac** and **Privilege Management for Unix and Linux.**

The BeyondTrust Privilege Management for Windows and Mac solution enables organisations to remove local admin rights, enforce control over what users are permitted to install or run, and enable least privilege access to designated applications and processes. Privilege Management also enables deep forensics and compliance reporting across all user activity without impacting worker productivity or increasing management burdens.

Privileged Access Management (5.3)

"Privileged accounts on a network are prime targets for malicious exploitation because they usually have more authority and access to resources. An attacker who has access to these accounts could potentially move about in the network and access privileged resources to gain unauthorised and persistent access to the entire system. Therefore, privileged access must be subject to tighter access control and greater monitoring."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 5.3

Section 5.3 of the CCoP's Protection Requirements covers security controls and balances for privileged accounts, privileged access, and privileged activity monitoring within CII environments. Though it shares the same name as this section, BeyondTrust's Privileged Access Management platform offers an extensive array of capabilities that include, but also extend beyond the listed requirements of this section.

As it relates to the requirements of section 5.3, BeyondTrust once again can help organisations satisfy a significant amount of the core requirements outlined in the CCoP document. Enforcing rigorous security across privileged access, permissions, and remote access connections are key functions at the heart of the BeyondTrust PAM platform.

BeyondTrust Password Safe helps CIIs gain a complete understanding of all the privileged accounts across environments and bring them under control. This is done via the Automatic discovery and onboarding of accounts. In addition, credentials associated with these accounts can be stored, managed, and rotated as needed, eliminating embedded credentials in scripts and code.

Password Safe offers integrations with leading MFA applications, allowing organisations to enforce additional step-up authentication on privileged accounts. In instances where additional permissions are needed after initial log-in, BeyondTrust Privilege Management for Windows/Mac or Privilege Management for Unix/Linux can provide the appropriate path. It can also enforce access policies to allow connections only from restricted IP addresses.

Network Segmentation & IT/OT (5.5)

"Network segmentation is the separation of a network into different segments based on their security and risk levels, and controlling communication between them."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 5.5

Once an impossibility, the remote access of operational technology (OT) is becoming more common place in today's information landscape. However, it is important to ensure OT access is executed in a secure manner that maintains sealed security of the separate systems.

Using BeyondTrust **Privileged Remote Access** as a replacement to your corporate VPN for operators, suppliers, or third-party vendors to access OT environments eliminates remote access blind spots, reduces the attack surface, and drives productivity. Because of its secure design, Privileged Remote Access allows you to maintain logical and physical network separation for remote access to operational technologies, in compliance with the Purdue model.

Additionally, BeyondTrust Privileged Remote Access allows operators of CII to enforce least privilege during remote access sessions. The solution provides application access independent of network access and enables API security to protect the integrity of data being sent from IoT devices to back-end systems.

Remote Connection (5.7)

"Remote connection is the access to a non-public computing resource by a user (or a process acting on behalf of a user) communicating through an external network."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 5.7

This section of the Code emphasises the importance of secure remote access within Critical Information Infrastructure, particularly in the context of performing "administration or maintenance from an external network".

While the requirements of this section of the code don't entirely rule out Virtual Private Networks (VPNs), earlier sections of the Code that outline Governance Requirements around least privilege and zero trust would preclude many implementations of VPNs. Even where a VPN may be configured to meet zero trust requirements, the processes involved with configuring networking routing require significant resources to stand up a single account and can heavily impact productivity.

BeyondTrust **Privileged Remote Access** seamlessly integrates with external user directories, such as Active Directory, for simple and secure privileged user management. In addition, it can also be connected to a supplier's Federated Identity Provider (IdP) to provide seamless onboarding and offboarding of user accounts, if desired. BeyondTrust solutions also enable seamless Single Sign-On (SSO) for frictionless onboarding.

User credentials can be masked, ensuring that should a user or third-party leave the organisation's employment, they no longer have access. Importantly, this solution also offers granular access controls. This enables alignment to the principle of least privilege, including restricting access to specified endpoints only, time-based access, and preventing unauthorised applications from being viewed. Multi-factor authentication can be integrated to meet the requirement within the CCoP while BeyondTrust enforces SSL for every connection.

Additionally, session logging allows for the review of all end system and network interactions. This log includes users involved, which endpoints they connected to, and system information. BeyondTrust Privileged Remote Access also records each session. These recordings capture every action taken in each remote desktop, SSH, or Telnet session.

System Hardening (5.9)

"Servers, consoles, workstations, appliances, network devices and field devices, in their default state, are not secured. Unnecessary services and programs are often left unmonitored, and they are potential avenues for a cyber threat actor to exploit. System hardening measures reduce the likelihood for the cyber threat actor to exploit vulnerabilities on assets that could lead to the compromise of the CII."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 5.9

As Section 5.9 within the Code points out, the default state for many endpoints and devices connected to networks is often highly unsecure. In most cases, these systems are running unauthorised applications, scripts, and more, all increasing the total threat surface of the organisation. Traditional application allowlisting may be challenging to implement, be highly time-consuming, and may significantly impact employee productivity. This is where a modern PAM approach significantly improves outcomes – including those provided by BeyondTrust **Privileged Access Management.**

Within the BeyondTrust platform, **Privilege Management for Windows and Mac** and **Privilege Management for Unix and Linux** solutions can quickly remove all admin and superuser accounts, instead assigning just-in-time (JIT) privileges only to approved applications, scripts, tasks, and commands. This allows Critical Information Infrastructure operators to strike a balance between security and productivity, while also reducing the volume of service desk calls by automatically elevating a user's privileges to trusted apps.

By leveraging BeyondTrust's QuickStart policy templates, asserting this control over applications can be done in a matter of hours instead of months. QuickStart is unique in the industry, allowing you to remove admin rights overnight. BeyondTrust Privilege Management deploys across your Windows, macOS, Unix, and Linux environments to restrict the use of executables, scripts, installers, control panel applets and the installation of approved drivers.

Both Privilege Management solutions also include the ability to implement effective allow and denylisting with flexible, configurable options in between, allowing you to prohibit unknown applications from executing (if required). This approach significantly reduces your organisation's attack vector and mitigates 70% of the critical vulnerabilities in the Windows operating system.

Administrators also have access to a rich set of preconfigured dashboards and reports for executed applications, elevated applications, blocked applications and discovered applications. The latter provides a breakdown of the applications in an environment, allowing administrators visibility into what is being used within the organisation and any systems that may require attention.

BeyondTrust **Password Safe** allows Critical Information Infrastructure operators to securely manage and store credentials for privileged accounts. These can be rotated to meet the exact policies of the organisation, including rotating every time they are used. Furthermore, credentials can be masked so that users never know them.

The CCoP also notes that malware protection needs to be kept up to date with the latest signatures. However, as malware detection has improved, threat actors have evolved their techniques to include "living off the land" attacks, which can be missed by malware detection solutions.

BeyondTrust's **Privilege Management for Windows and Mac** offers trusted application protection, a feature designed to thwart these attacks by understanding the context in which system processes should or should not run, including system tools such as PowerShell. This capability helps to protect the everyday trusted applications – such as Microsoft Word, Excel, or Outlook – your users utilise most frequently from attacks by providing additional malware coverage on top of the standard tools.

Patch Management (5.10)

"Timely application of security patches limits the opportunity for a cyber threat actor to exploit vulnerabilities. Hence, it is important for organisations to monitor for new vulnerabilities and their corresponding security patches, and to develop procedures to prioritise and apply the security patches promptly."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 5.10

Effective patch management is a key defence measure within any organisation's security strategy. Limiting the window of opportunity that threat actors can take advantage of vulnerabilities identified in systems and software is paramount. This section of the Code makes note of this fact and details several requirements to meet its definition of a compliant security patch management process.

While BeyondTrust does not directly manage the administration of patching, the Code notes that CIIs need to apply compensating controls to mitigate and reduce risks where a patch cannot be applied. BeyondTrust's **Privilege Management for Windows and Mac** and Privilege Management for Unix and Linux solutions allow cybersecurity teams to block vulnerable versions of applications from running on endpoints until a patch can be applied.

Application Security

"Attackers can potentially use many different paths through the applications used in the CII environment to do harm to the CIIO's businesses or organisation. As such, application security which describes cybersecurity measures and practices at the application level should be adopted to secure the application code and data."

- Cybersecurity Code of Practice for Critical Information Infrastructure, Section 5.12

This section of the CCoP reiterates the need for CII operators to have control over the applications that are installed and run in the environment. Operators must create and maintain the list of approved applications.

BeyondTrust **Privilege Management for Windows and Mac** and Privilege Management for Unix and Linux provide control over the applications that can be installed and run by users.

Security policies can be applied to groups of users who need more flexibility, such as developers, to have additional capabilities to run applications over other groups whose needs are more restrictive. Exception handling, such as requests to run applications that fall outside of the approved list, can be escalated. For example, via an integration with an ITSM or ticketing solution like ServiceNow for review, logging, and approval.

Operational Technology (OT) Security Requirements

Within Section 10 of the *Cybersecurity Code of Practice*, there are additional specific requirements listed regarding securing access to and hardening the security of Operational Technology architectures.

Notably, the Code's guidance highlights that increasing connectivity between IT and OT systems provides new avenues for attackers to move laterally between systems. Connections between OT and IT systems should therefore be minimised to only what is necessary while accounts and credentials should not be shared between environments.

With the Code calling on operators of CII to limit the connections between OT and IT systems, it is important to note that the architecture of the BeyondTrust Privileged Remote Access solutions allows for adherence to the Purdue model, which provides a framework for segmenting OT from corporate networks.

To limit the ability for attackers to leverage compromised credentials from IT in OT environments, the CCoP also requires separate authentication mechanisms and credentials for OT users to accounts on the IT network. Privileged Remote Access provides this capability, whether users are employees of the operator or third-party suppliers.

Credential injection and obfuscation via the in-built vault or another vaulting solution, such as BeyondTrust Password Safe, means that credentials needed for privileged access are never displayed to the user. This extra level of security protects the environment from potential lateral movement and makes it difficult for operators to bypass controls enforced by the PAM platform, such as approval processes, audit logging and session recording.

BeyondTrust Privileged Remote Access also provides a full audit trail and records all sessions to facilitate investigations into what actions any user account took. In addition, integrations with solutions such as Splunk allow for greater visibility into activity across your infrastructure to identify potential threats or attacks, meeting the needs of the CCoP in monitoring OT data flows for anomalies and providing a trigger when detected.

Conclusion: The BeyondTrust Platform & the CCoP

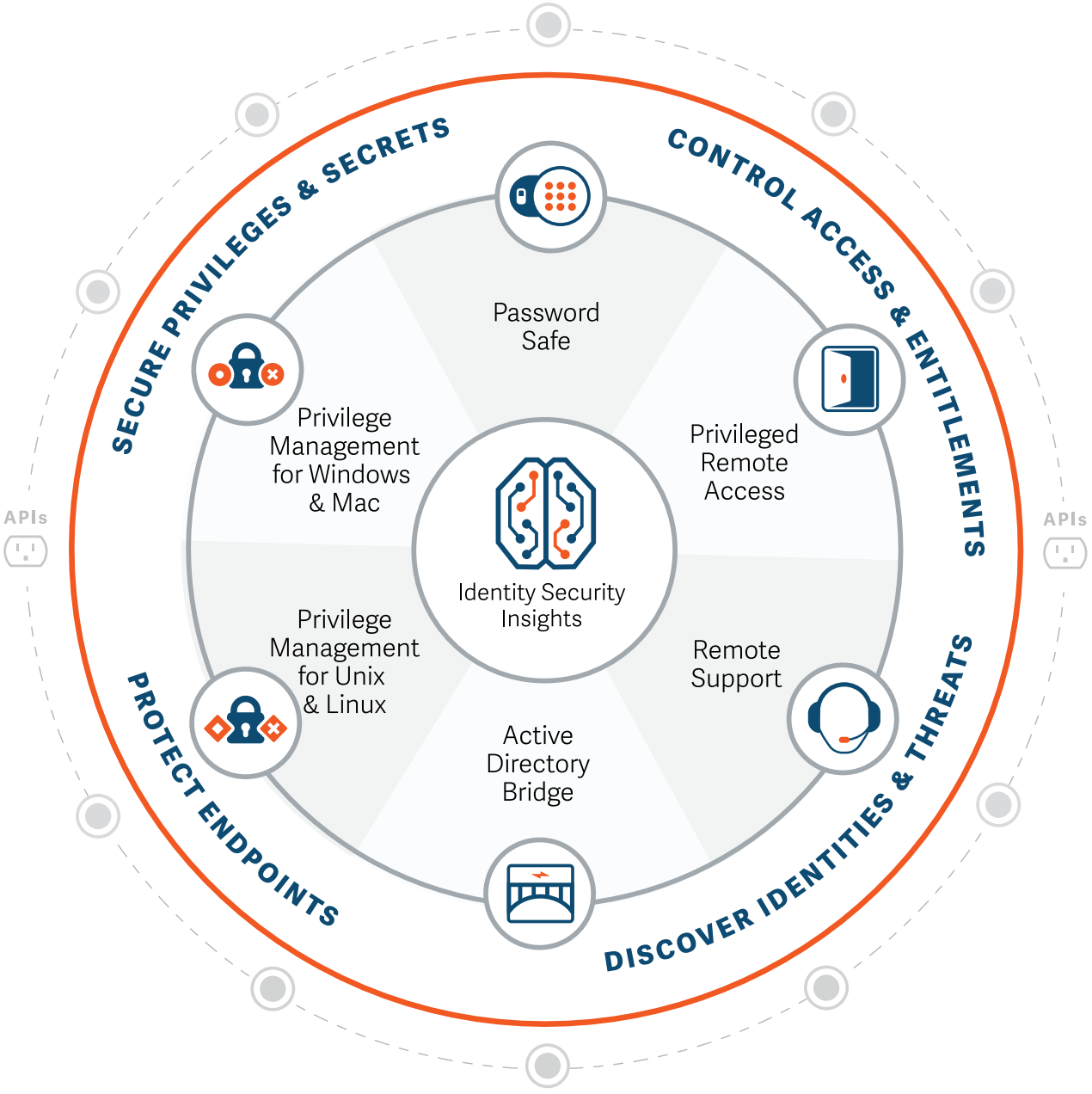
The **Cybersecurity Code of Practice for Critical Information Infrastructure** issued by the Cyber Security Agency of Singapore contains sweeping requirements for organisations operating within Singapore to improve their cybersecurity resiliency and comply with modern cybersecurity standards. Just as with similar guidelines and frameworks issued around the world, BeyondTrust Privileged Access Management solutions satisfy a significant amount of these security requirements and offer capabilities beyond the scope of other solutions on the market.

The BeyondTrust platform helps to implement the secure foundation organisations need to enable remote work and digital transformation, all while remaining resilient, adaptive, and highly protected from modern cyberthreats.

Why Partner with BeyondTrust to Meet CCoP Requirements?

- BeyondTrust is the only product vendor to address all Privileged Access Management use cases. Our comprehensive solution includes substantive capabilities no other vendor delivers.
- Our next-generation capabilities extend your line-of-sight to privileged threat pathways and identity-based attack chains, well beyond the capabilities offered by other solutions on the market.
- The breadth of our solutions and the flexibility of our offerings enable you to handle today's threat scenarios and prepare for tomorrow's possibilities.
- You can choose from the deployment model that best suits your needs – including cloud, virtual, or on-premises appliances. No other PAM vendor provides more choices.

The BeyondTrust Platform



Password Safe

Manage privileged passwords, accounts, keys, secrets, and sessions for people and machines; and secure non-privileged employee passwords for business applications.

Privileged Remote Access

Extend privileged access security best practices beyond the perimeter by granularly controlling, managing, and auditing remote privileged access for employees, vendors, developers, and cloud ops engineers.

Privilege Management for Unix & Linux

Achieve compliance, establish least privilege and zero trust, and prevent and minimise security breaches — without hurting productivity.

Privilege Management for Windows & Mac

Remove local admin rights, enforce least privilege dynamically across Windows and macOS, prevent malware and phishing attacks, and control applications without compromising productivity.

Identity Security Insights

Gain a centralised view of identities, accounts, entitlements, and privileged access across your IT estate and detect threats resulting from compromised identities and privileged access misuse.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners. Learn more at **beyondtrust.com**