An Actionable Guide to Achieving Compliance with Malaysia Risk Management in Technology (RMiT)

Utilising BeyondTrust Solutions for Privileged Access Management and Vulnerability Management

WHITEPAPER

February 2019

Introduction

Cybercriminals have long sought to exploit technological vulnerabilities to gain access to sensitive electronic data and financial transactions. With this access, they can cause significant financial losses for any entity or consumer whose private information may be revealed or stolen for illicit purposes. The financial services industry is a significant target for cyber threats due to immediate monetary gain.

Given the severity of the issue and the risk to all regulated entities, certain minimum standards are warranted. The Malaysian Risk Management in Technology (RMiT) is a framework meant to combat the ever-growing threat posed to information and financial systems by nation-states, terrorist organisations, and independent criminal actors. This regulation is designed to:

- Promote the protection of customer information
- Promote the protection of information technology systems of regulated entities
- Require each company to assess its specific risk profile
- Design a program that addresses its risks in a robust fashion
- Certify compliance with these regulations by senior management

Utilising RMiT Guidance for Bank Technology Security

In keeping with Bank Negara Malaysia's recommendations, BeyondTrust encourages all financial entities to act promptly to adopt a cybersecurity program that meets these objectives. BeyondTrust solutions can help organisations meet the requirements set forth in RMiT BNM/RH/ED 028-11. This white paper demonstrates how BeyondTrust solutions can address these requirements. Please see the table on the following pages of this paper for detailed mapping of the BeyondTrust solutions into RMiT requirements.

MAPPING BEYONDTRUST SOLUTIONS TO RMIT REQUIREMENTS

Title / Section	Description	BeyondTrust Solution
Access Control		
10.79	A financial institution must establish an effective access control policy to manage the risk of unauthorised access to its technology systems. The access control policy must include logical and physical technology access controls of its users (including external users, e.g. third-party service providers), technology systems and technology assets.	The BeyondTrust Privileged Access Management (PAM) Platform includes remote access and privileged access solutions using protocol-based jump host technology to broker connectivity to sensitive systems and enforce effective access control policies for internal and external users.
10.80	A financial institution must reflect the following principles in its access control policy: (a) Adopt a "deny all" access control policy for users by default unless explicitly authorised; (b) Enforce "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; (c) Employ time-bound access rights which restrict access to a specific period including access rights granted to service providers; (d) Employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to	The BeyondTrust PAM Platform includes the following technology to address these requirements: (a) Privileged access to sensitive systems is denied by default unless explicitly allowed. (b) Endpoint privilege management solutions to enforce least privilege on Unix, Linux, Windows, MacOS, and network devices. (c) BeyondTrust policies are context-aware and support geolocation, IP ranges, and time-based access rights. (d) BeyondTrust solutions support advanced workflows and approval processes for access and commands in order to ensure no single person has authoritative access to systems and circumvent proper roles and responsibilities.

Title / Section	Description	BeyondTrust Solution
	independently modify, circumvent, and disable system security features such as— (i) System development and technology operations; (ii) Security administration and system administration; and (iii) Network operation and network security. (e) Enforce dual control functions which requires two or more persons to execute an activity; (f) Adopt stronger authentication for critical activities including for remote access; (g) Prohibit use of same user ID for multiple concurrent sessions; (h) Prohibit sharing of user ID and passwords across multiple users; and (i) Restrict the use of generic user ID naming conventions in favour of more personally identifiable IDs.	(e) BeyondTrust solutions support multiple approver and workflow use cases. (f) BeyondTrust remote access and privileged access solutions support multi-factor and two-factor solutions. (g) BeyondTrust privileged access solutions can limit and manage credentials used for concurrent sessions. (h) BeyondTrust privileged access solutions can instantiate single usage for all credentials to prevent sharing. (i) Not applicable.
10.83	A financial institution shall continuously review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords.	The BeyondTrust PAM Platform is capable of automatically rotating and storing passwords based on a password complexity policy implemented by an administrator. This ensures best practices are

Title / Section	Description	BeyondTrust Solution
	There must be a mechanism to automatically generate passwords and to check the strength of the passwords created manually.	always enforced and minimum strength is always adhered to.
10.89	A financial institution must not allow remote access by default. Should remote access be required and granted, the principles outlined in paragraph 10.80 must be applied.	The BeyondTrust PAM Platform includes secure remote access and privileged access technology to ensure sessions are monitored, managed, and that default remote access is never granted.
10.90	A financial institution must ensure all user activities are logged and periodically reviewed.	The BeyondTrust PAM Platform includes complete session monitoring, keystroke logging, and command indexing to document all user activity and facilities to document that sessions are periodically reviewed.
10.91	In addition to the requirement under paragraph 10.90, large financial institutions are required to deploy automated audit tools to flag any anomalies.	The BeyondTrust PAM Platform includes advanced threat detection policies, analytics, and third-party event integration to detect anomalies and provides audit tools based on indicators of compromise.
Patch and End-of-Life System Management		
10.92	A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems.	The BeyondTrust PAM Platform includes vulnerability management that can identify end-of-life operating systems and assets.
10.93	A financial institution must establish functions to continuously monitor and implement latest patch releases in a timely manner and identify critical technology systems that are approaching EOL for further remedial action.	The BeyondTrust PAM Platform contains continuous vulnerability assessment technology, Windows patch management, and detailed reports to prove the service level agreements for security updates required, in a timely fashion.

Title / Section	Description	BeyondTrust Solution
10.94	In fulfilling the objective under paragraph 10.93, large financial institutions must establish a dedicated function.	The BeyondTrust PAM Platform includes enterprise-ready vulnerability management for the largest organisations in the world.
10.95	A financial institution must establish a patch and EOL management framework which outlines amongst others the following: (a) Identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems; (b) Conduct compatibility testing for critical patches; (c) Specified turnaround time according to the severity of the patches; and (d) Workflow of end-to-end patch deployment processes including approval, monitoring and tracking of activities.	BeyondTrust Enterprise Vulnerability Management includes the following capabilities to address these requirements: (a) Network and agent-based vulnerability assessment to identify risks from undeployed patches, zero-day threats, and EOL systems. (b) Not applicable. (c) Provide SLA reports to measure the turnaround time of successful patch deployments. (d) Integrate with ticketing and patch management systems to provide end-to-end workflows for patch deployments, including approval, monitoring, and tracking of activities.
Cybersecurity Operations		
11.7	A financial institution must enable continuous and proactive monitoring and deploy advanced tools to timely detect anomalous activities in its technology infrastructure. The scope of monitoring must be extensive to cover all critical technology applications and systems including its supporting infrastructure.	The BeyondTrust PAM Platform includes advanced technology for continuous proactive monitoring and anomaly detection of privileged access, remote access, password management, and least privilege via analytics, reports, and third-party event integration.
11.8	A financial institution must continuously assess its security	The BeyondTrust Enterprise Vulnerability Management solution

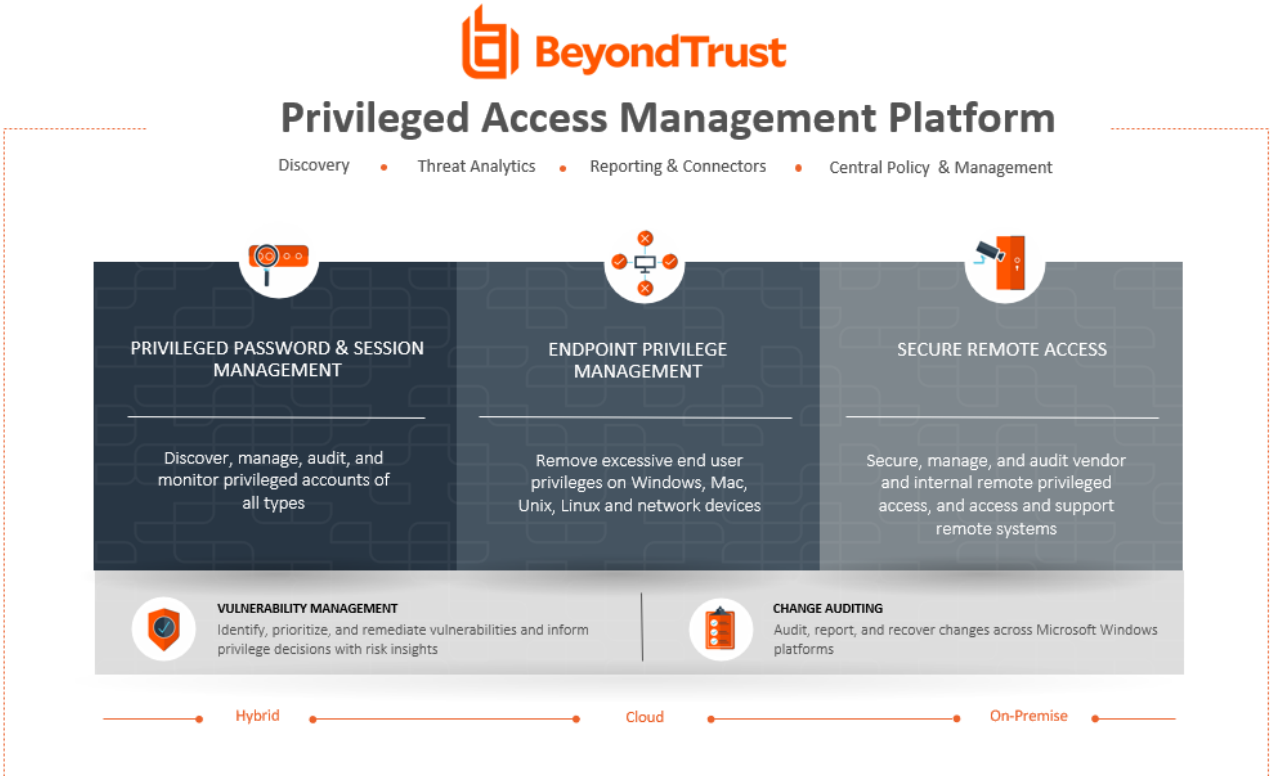
Title / Section	Description	BeyondTrust Solution
	posture to provide reliable assurance of its resiliency against sophisticated threats and vulnerabilities.	includes continuous vulnerability assessment technology to measure the security posture of the organisation from sophisticated threats and inappropriate asset changes.
11.12	A financial institution must establish standard operating procedures (SOP) for vulnerability assessment and penetration testing (VAPT) activities. The SOP must spell out the relevant control measures including ensuring the external penetration testers are accompanied in-premise at all times, validating the event logs and ensuring data purging.	BeyondTrust Enterprise Vulnerability Management adheres to industry standards for operating a vulnerability assessment solution. In addition, BeyondTrust provides a SOP for organisations looking to formalise the procedures and processes around vulnerability management, including data retention and audit findings.
Security Operations Centre (SOC)		
11.20	A financial institution must also ensure the following functions are performed to further enhance the SOC's capabilities: (a) Vulnerability management including conducting vulnerability assessment, penetration testing and threat hunting; (b) Remediation functions including ability to perform forensics artefact handling, malware and implant analysis; and (c) Provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, monitoring	The BeyondTrust PAM Platform includes the following capabilities in support of this requirement: (a) The BeyondTrust Enterprise Vulnerability Management performs vulnerability assessment and assists with threat hunting. (b) The BeyondTrust PAM Platform can assess running processes for malware using BeyondInsight Clarity. (c) The BeyondTrust PAM Platform includes BeyondInsight Clarity that provides threat intelligence, indicators of compromise, and behavioural analytics.

Title / Section	Description	BeyondTrust Solution
	indicators of compromise (IOC). This includes advanced behavioural analysis to detect signature-less malware or identify anomalies that may pose security threats.	
Appendix 5 – Minimum Control Measures on Cybersecurity		
2.	Update checklists on the latest security hardening of operating systems.	BeyondTrust Enterprise Vulnerability Management includes a SCAP based configuration compliance assessment engine with the latest security hardening templates to verify operating system and application security hardening.
3.	Update security standards and protocols for web services encryption regularly. Disable support of weak ciphers and protocol in web facing applications.	The BeyondTrust Enterprise Vulnerability Management solution is capable of network-based assessments on assets and applications to identify and report on weak ciphers and expired certificates.
6.	Ensure security controls for remote access to server include the following: (a) Restrict access to only hardened and locked down end-point devices; (b) Use secure tunnels such as TLS and VPN IPSec; (c) Deploy 'gateway' server with adequate perimeter defenses and protection such as firewall, IPS and antivirus; and (d) Close relevant ports immediately upon expiry of remote access.	The BeyondTrust PAM Platform contains the following capabilities in support of remote access: (a) BeyondTrust Privileged Access and Remote Access technologies can assess and restrict access to properly hardened hosts. (b) Supports strong encryption and secure protocols for access. (c) Utilises a gateway or jump server for remote access, including full session monitoring. (d) Secures access using a dedicated client so no open ports are exposed.

The number of cyber events has been steadily increasing and estimates of the potential risk to the financial services industry are irrefutable. Adoption of this cybersecurity program and standardisation on policies and procedures is the only way to ensure the security of financial systems within Malaysia. BeyondTrust solutions for Privileged Access Management and Vulnerability Management can help organisations to meet the requirements set forth in RMiT.

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management Platform is an integrated solution that provides control and visibility over all privileged accounts and users. By uniting capabilities for password and session management, endpoint privilege management, secure remote access, and vulnerability management that many alternative providers offer as disjointed tools, the platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privilege risks.



About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access.

Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralized management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments.

BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 500, and a global partner network. Learn more at beyondtrust.com