WHITEPAPER

Addressing the MAS TRM with Privileged Access Management

How BeyondTrust can help you meet key mitigation strategies

BeyondTrust

Table of Contents

Overview of the Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines 2021

The technology landscape of the financial sector is transforming at an increasingly rapid rate as financial services organisations look to take advantage of the operational efficiencies and cost savings that digital transformation offers. However, the underlying information technology (IT) infrastructure supporting financial services has grown in scope and complexity, increasing their cyber security exposure.

With increasingly sophisticated attacks targeting the weak links in the interconnected financial ecosystem, each organisation needs to understand their cyber security exposure and put in place a robust risk management framework to ensure IT and cyber resilience.

The revised MAS Technology Risk Management Guidelines in January 2021 set out technology risk management principles and best practices for the financial sector, to guide FIs in establishing sound and robust technology risk governance and oversight and maintaining cyber resilience. They aim to promote the adoption of sound and robust practices for the management of technology risk.

Achieving Compliance with BeyondTrust PAM Solutions

BeyondTrust solutions can help enterprises meet the requirements in the MAS TRM by addressing the following:

BeyondTrust Solutions Mapped to the MAS Guidelines

Section	Description	BeyondTrust Solution
4 Technology Risk Management Framework		
4.4 Risk Treatment	4.4.1 The FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance.	BeyondTrust's Privileged Access Management solutions provide the ability to put in place controls based on end-user roles and organizational responsibilities. This provides separate, auditable, documented policy sets and individual end user interaction with IT & IS resources.
4.5 Risk Monitoring, Review and Reporting	4.5.1 The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks. 4.5.2 A risk register should be maintained to facilitate the monitoring and reporting of technology risks.	BeyondTrust Privileged Access Management solutions help organizations implement automated controls for generating, protecting, and reviewing audit records based on all privileged user, asset, and application activity. This includes:

		• Verification of audit, accountability, and privileged workflow procedures implemented in the solution • Detailed audit events for privileged activity and privileged credential usage • Tamper protection to ensure audit records are accurate • Automatic notification and correction of faults when collecting logs or audit data related to the system • Detailed reporting and indexing of audit data with anomaly and behavioural detection • Time stamp and detailed audit information to perform required analysis for regulatory compliance or determine if there is an indicator of compromise • Configurable audit log retention parameters to adhere to local, regional, industry, or government regulatory policies
6 Software Application Development and Management		
6.3 DevSecOps Management	6.3.2 The FI should implement adequate security measures and enforce segregation of duties for the software development, testing and release functions in its DevSecOps processes.	The BeyondTrust solution for enabling secure DevOps reduces risks throughout the IT supply chain by improving visibility and control over secrets and admin privileges. By uniting these capabilities across on-premise, virtual, cloud, and DevOps use cases, information technology teams can better achieve their agility goals, while driving more value from their existing security investments.
6.5 Management of End User Computing and Applications	6.5.2 The FI should establish measures to control and monitor the use of shadow IT in its environment. 6.5.3 A process should be established to assess the risk of end user developed or acquired applications to the FI and ensure appropriate controls and security measures are implemented to	BeyondTrust Endpoint Privilege Management for Windows, Mac & Unix/Linux removes excessive end user privileges and controls for applications on Windows, Mac, Unix, Linux, and networked devices without hindering end-user productivity. This ensures that users have the right amount of privileges to be productive but cannot install unapproved software.

	address the identified risks, and approval is obtained before being used.	BeyondTrust Endpoint Management provides trust-based application whitelisting ensuring that users retain the flexibility they need to be productive while being secure. It allows listing, block listing, and grey listing to help ensure only legitimate approved applications are allowed, reducing the threat surface, and enabling productivity.
9 Access Control		
9.1 User Access Management	9.1.1 The principles of 'never alone', 'segregation of duties', and 'least privilege' should be applied when granting staff access to information assets so that no one person has access to perform sensitive system functions. Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers.	BeyondTrust Privileged Access Management solutions provide several methods to support the controlled implementation of policies, along with technology to manage policies through a change control and deployment life cycle. In addition, BeyondTrust solutions incorporate role-based access control policies to limit and restrict access to only authorized users. BeyondTrust Privilege Remote Access ensures that remote users can access only the resources/application required with tight real time supervision and audit.
	9.1.2 The FI should establish a user access management process19 to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner.	BeyondTrust solutions allow the administrator to set up time and location-based policies to ensure that users can only access resources from a designated location for a pre-determined duration. Out of bound access with workflow adds additional level of security.
	9.1.3 For proper accountability, the FI should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes.	BeyondTrust solutions allow granular access policies and audit capabilities. All access is logged and is available for video replay. BeyondTrust's Privileged Access Management solutions provides the ability to enforce policies based on end-user roles and organizational responsibilities. This provides separate, auditable, documented policy sets and

		individual end user interaction with resources throughout an enterprise.
9.2 Privileged Access Management	9.2.1 Users granted privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment. Access to privileged accounts should only be granted on a need-to-use basis; activities of these accounts should be logged and reviewed as part of the FI's ongoing monitoring.	BeyondTrust's Privileged Access Management solutions provide native workflow capabilities and integrations into existing ITSM solutions to ensure proper authorization is granted before a user is provided access. These capabilities include: • Workflows requiring multiple approvals such that two or more individuals must approve user access before granting permissions. • Security-relevant information is logged during all access attempts and can be forwarded to other solutions of authority. • Role-based access control based on IAM integrations, Active Directory, LDAP, and on native RBAC models. Revocation of access authorization based on context or suspicious activity. • Secure remote access internally or externally based on context or just in time requirements. • Access control restrictions to limit lateral movement or attempts to exfiltrate data. • Enforcement of least privilege even when assigned tasks require administrative rights.

	9.2.2 System and service accounts are used by operating systems, applications and databases to interact or access other systems' resources. The FI should establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.	BeyondTrust's Privileged Access Management solutions helps secure service and system accounts used for application-to-application access. BeyondTrust eliminates hard-coded or embedded application credentials automatically, simplifying management for IT and better securing the organization from exploitation of those credentials. • Enables removal of hard-coded passwords from applications and scripts • Provides an extensible REST interface that supports many languages, including C/C++, Perl .NET, and Java • Ensures that passwords can be automatically reset upon release • Enforces extensive security controls to lock down access to only authorized applications
9.3 Remote Access Management	9.3.1 Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment. 9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been secured according to the FI's security standards.	BeyondTrust Secure Remote Access enforces a policy of least privilege by giving users just the right level of access needed for their roles with individual accountability for shared accounts. Allows administrator to define what endpoints users can access, schedule when they can access them, and whitelist / blacklist applications for a comprehensive approach to privileged remote access. It allows easy control and monitoring of sessions via a secure agent or using standard protocols for RDP, VNC, Web, and SSH connections. You can also set authorization and notification preferences to be alerted when a user is accessing BeyondTrust Privileged Remote Access. Administrators can use their mobile devices to approve requests and monitor access usage from anywhere.

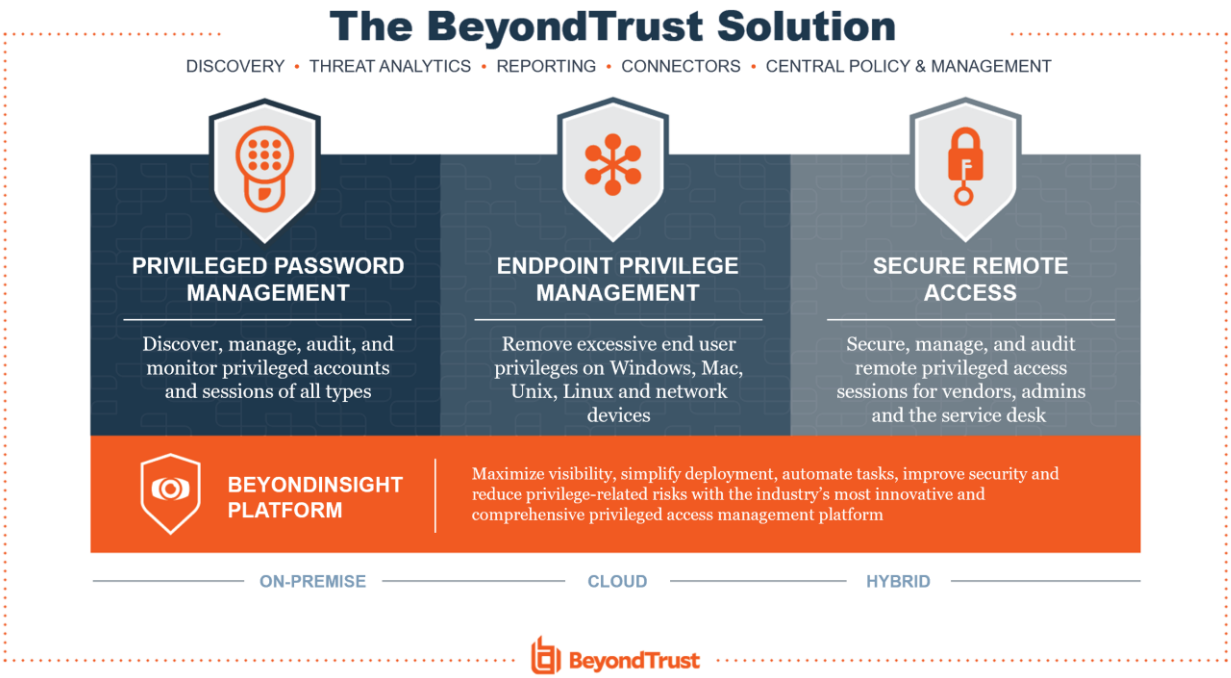
		BeyondTrust Secure Remote Access can address these privileged access security gaps in the Cloud by providing a layer of security for authenticating to these systems with full session monitoring capabilities. In addition, it allows secure connections to resources remotely and automatically inject secure credentials—completely invisible to the end-user and without ever revealing the password—to access those resources in a controlled manner.
11 Data and Infrastructure Security		
11.1 Data Security	11.1.1 The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data	BeyondTrust solutions provide the ability to restrict pivoting commands and ensure that the user cannot run harmful commands or commands that allow lateral movement.
11.2 Network Security	11.2.2 To minimise the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets.	BeyondTrust solutions provide the ability to restrict pivoting commands and ensure that the user cannot run harmful commands or commands that allow lateral movement.
11.3 System Security	11.3.3 Endpoint protection, which includes but is not limited to behavioural-based and signature-based solutions, should be implemented to protect the FI from malware infection and address common delivery channels of malware, such as malicious links, websites, email attachments or infected removable storage media.	BeyondTrust Endpoint Privilege Management removes local admin privileges and applies least privilege access across all users, applications, and systems to stop many ransomware attacks. It will also mitigate the impact of those ransomware payloads that do gain a foothold in your environment by closing down lateral pathways and reducing the ability to elevate privilege. Least privilege can even mitigate the impact of stolen credentials. If the credentials are for a user, endpoint, or application with limited or no privileges/privileged access, then the damage can also be diminished.

	11.3.6 Security measures, such as application whitelisting, should be implemented to ensure only authorised software can be installed on the FI's systems.	BeyondTrust Endpoint Privilege Management for Windows, Mac and Unix/Linux removes excessive end user privileges and application controls on Windows, Mac, Unix, Linux, and networked devices without hindering end-user productivity. This ensures that users have the right amount of privileges to be productive but cannot install unapproved software. BeyondTrust Endpoint Privilege Management provides trust-based application whitelisting ensuring that users retain the flexibility they need to be productive while being secure. It allows whitelisting / blacklisting, and grey listing helps ensure only legitimate approved applications are allowed, reducing the threat surface and enabling productivity.
	11.3.7 When implementing Bring Your Own Device (BYOD), the FI should conduct a comprehensive risk assessment and implement appropriate measures to secure its BYOD environment before allowing staff to use their personal devices to access the corporate network.	BeyondTrust Secure Remote Access allows enterprises to provide secure connectivity to enterprise resources while granularly defining the endpoint or resource the user is accessing. It provides the ability to perform the connection through a web browser without the need for VPN software, dedicated applications, nor protocol tunnelling.
11.5 Internet of Things	11.5.4 The FI should implement controls to prevent unauthorised access to IoT devices.	BeyondTrust Privileged Remote Access allows enterprise to grant secure access to their IOT devices from within and outside their enterprise in a controlled and auditable manner.

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.