A RICOH Company

Managed CyberArk PAM Service Definition Document

Ref no: G Cloud 15 Version 1.0

PREPARED FOR

G Cloud 15

PREPARED BY

MTI Technology Ltd

info@mti.com
www.mti.com

1 Document Usage

Paper copies are not controlled.

2 Revision and Review History

2.1.1 Amendment record

Issue Status	Version	Date	Actioned By	Description
Release	V 1.0	28/01/2026	Kevin Foster	Finalisation & Issue for G Cloud 15

2.1.2 Confidentiality Statement

All information contained in this document is Restricted. No copies or external distribution permitted without the consent of the document owner, or MTI's Board of Directors.

info@mti.com
www.mti.com

Contents

info@mti.com
www.mti.com

3 Introduction

CyberArk Privileged Access Management (PAM) secures the keys to your IT kingdom. With CyberArk protecting your privileged accounts across your environments, maximising your investment and protection by ensuring the solution runs in an efficient and reliable manner is critical. MTI's PAM Managed Services leverage over 15 years' experience of Privileged Access Management (PAM) and CyberArk, with end-to-end project experience in CyberArk solution architecture, deployment, integration, upgrades and migration to provide the support and management expertise to ensure the CyberArk environment runs smoothly and efficiently meeting your business' needs.

MTI's PAM Managed Services are offered on a 9 x 5 basis with P1 and P2 support 24 x 7 x 365 as standard.

4 Support Service Overview

4.1 In-Scope Service Features

MTI's SLA backed CyberArk PAM Managed Service for *CyberArk PAM Self-Hosted* on-premises platform provides the following service to G Cloud 15 customers:

CyberArk PAM Managed Service

- ✓ 24 x 7 x 365 Priority 1 & Priority 2 CyberArk support
- ✓ In-hours support 09:00 – 17:00 GMT, Mon to Fri (excluding UK Bank Holidays)
- ✓ 9 x 5 SLA Backed Service
- ✓ MTI In-house CyberArk Certified Support Team
- ✓ Incident Remediation
- ✓ Major Incident Management
- ✓ Change Management
- ✓ Problem Management
- ✓ Email, Telephone, MS Teams and Remote Support
- ✓ Vendor Escalation
- ✓ Tailored Security Bulletin Notification and Applicability and Guidance
- ✓ Operational Guidance on CyberArk Platform
- ✓ Priority Case Handling
- ✓ Bi-Annual Remote Health Checks (including Report of New Releases and Features Available & Review of Un-used Functionality with Recommendations)
- ✓ Checking Vault backups are configured via PAReplicate tool and running correctly
- ✓ Proactive Monitoring of CyberArk Application and Web Service (CPM, PSM, PVWA etc.)
- ✓ 1 x Annual upgrade of in-situ CyberArk Component Servers
- ✓ Unlimited CyberArk Component Server Patching
- ✓ Unlimited Patching of the CyberArk Vaults
- ✓ Scheduled Privileged Account Discovery Scans
- ✓ Adding / Amending / Removing Directory Mappings
- ✓ Adding / Amending / Removing Safes
- ✓ Adding / Amending / Removing Safe Members
- ✓ Adding / Amending / Removing Accounts
- ✓ Adding / Amending / Removing 'Out of the box' Target Platforms
- ✓ Adding Accounts and Creating New Templates
- ✓ Mapping Existing or New Groups to CyberArk Safes
- ✓ User Directory Role Base Access Control Mapping
- ✓ New Directory Role Base Access Control Mapping

- ✓ Managing CyberArk policy & password changes
- ✓ CyberArk System Health & Access Alerting
- ✓ Monthly (Remote) Service Delivery Manager Reviews
- ✓ Monthly CyberArk System Reports
- ✓ Monthly Service Reporting
  - Management Overview
  - CyberArk System Reports
  - Safe, accounts & user activity
  - Compliance
- ✓ 1 x Annual CyberArk Disaster Recovery Test

4.2 Annual Upgrade

The PAM Managed service includes for a fully qualified CyberArk engineer to perform an upgrade of all CyberArk PAM Self-Hosted software. MTI will notify you when an upgrade has been released and is suitable for your environment, along with the benefits of upgrading.

The upgrade is contingent on CyberArk having released an updated version of software for that year.

4.3 Responsive Support from Dedicated Specialists

One of the main reasons why customers choose MTI to provide Managed PAM Services is that our team of in-house CyberArk certified specialists are very experienced and responsive in managing PAM support cases. We use our own internal expertise to address the majority of issues and only escalate matters to CyberArk where there is a product limitation requiring their involvement. Performance against Service Level Agreements (SLA's) agreed with you is proactively managed to ensure you receive the response you are paying for.

The Customer will be allocated a dedicated Service Delivery Manager for the entire contract, who will be responsible for all elements of the Managed Service and will conduct regular service delivery review meetings.

4.4 Proactive Service

Our fully Managed customers receive a pro-active service; MTI let you know when important security and functionality patches are available and work with your change control processes to ensure they are applied in good time, either in or outside working hours as is needed (at no extra cost) to ensure your environment is securely maintained with no disruption to live service.

MTI proactively monitor your CyberArk environment to ensure it is running correctly at all times and work towards maintaining maximum uptime. We investigate alerts promptly, take required corrective actions and keep you informed of progress.

Service uptime is enhanced with our Bi-Annual Health Checks which proactively check for known issues to ensure they are addressed promptly. CyberArk system reports are also run monthly, and reviewed by a CyberArk specialist, before sending to the customer, highlighting any significant issues that require action, either by MTI, the customer or both parties.

Under the managed service, aside from keeping the CyberArk components fully functional we also look after all day-to-day activities such as adding new users, groups, safes, platforms etc. using simple, efficient change control request processes, aligned with our customer's change approval / CAB processes.

Scheduled Privileged Account Discovery Scans – to improve detection and onboarding of Privileged Target Accounts, MTI recommend scheduling regular privileged account discovery scans, to first identify new target accounts on monitored assets that are visible to the CyberArk deployment and then onboarding agreed human

operated accounts into CyberArk. Please see restriction in the section “Limitations to Service Scope” regarding onboarding of Service Accounts.

4.5 Proactive Monitoring Available where customer agrees (Customer Option)

Where agreed with the customer MTI will use mutually agreed Server Monitoring tooling to monitor the various CyberArk components for our managed service as listed below:

Main Vault – This will be configured to send SNMP traps to the monitoring tool with defined criteria. The monitoring tool is configured to send a notification to a defined email address when an SNMP trap is received.

DR Vault – This will be configured to send SNMP traps to the monitoring tool with defined criteria. The monitoring tool will then be configured to send a notification to a defined email address when an SNMP trap is received.

Password Vault Web Access (PVWA) – This will have the monitoring tool agent installed which will be configured to send an alert to the monitoring tool console when there are issues with certain services. Once the monitoring tool receives this alert it will send a notification to a defined email address. The monitoring tool is configured to periodically poll the main PVWA URL. If there is a problem connecting to this URL then a notification will be sent to a defined email address.

Central Policy Manager (CPM) - This will have the monitoring tool agent installed which will be configured to send an alert to the monitoring tool when there are issues with certain services. Once the monitoring tool console receives this alert it will send a notification to a defined email address.

Privileged Session Manger (PSM) - This will have the monitoring tool agent installed which will be configured to send an alert to the monitoring tool console when there are issues with certain services. Once the monitoring tool console receives this alert it will send a notification to a defined email address.

4.6 Supported Environment

This ***example*** Service definition document is based on remotely supporting **up to** following environment:

25 platforms

1 x Primary Vault

1 x Disaster Recovery Vault

1 x CPM	(Central Policy Manager)
2 x PVWA’s	(Password Vault Web Access)
2 x PSM’s	(Privileged Session Manager - Windows)
1 x PAReplicate	(Backup Utility)
2 x PTA	(Privileged Threat Analytics)

info@mti.com
www.mti.com

4.7 Service Level Agreement

4.7.1 Incident Priority Definition

Incident Priority	Definition
Priority 1	A down situation, whereby Client is unable to do production work, and a Work-Around is not available. This category includes situations where: • the protected server ceases to be operational. • the Software requires repeated reboots of the system.
Priority 2	A major function is unusable and no Work-Around is available, but the Client is able to do some production work. The Software may: • be usable but incomplete (one or more major documented commands / functions are inoperable or missing). • require rebooting of the system. • suffer sufficient degraded performance (throughput/response) such that there is a severe impact on use.
Priority 3	There is a loss of a function or resource that does not seriously affect Client's operations or schedules. Any problem, which was originally reported as a Critical Event or Serious event but has been temporarily solved with a Work-Around, will be reduced to a Moderate Event.

4.7.2 Incident Response Targets

Incident Priority	Target Response	Percentage Target
Priority 1	2 Hours	85% or above
Priority 2	4 Hours	85% or above
Priority 3	6 Hours	85% or above

4.7.3 Service Request Category Definitions

Category ID	Definition
SR Standard	All SR's listed under Appendix C, with the below exception where an SR has been deemed and accepted by both parties as urgent.
SR Urgent	Within the defined list of SRs under Appendix C, where a customer requests via the Service Delivery Manager that the SR is urgent for a business reason and the SDM chooses to accept.

4.7.4 Service Request Response Targets

Service Request	Target Response
SR Standard	4 Hours
SR Urgent	1 Hour

4.7.5 Support Hours

Resolver Function	In Hours Support	Remote Out of Hours Support	Physical Site Visit
Service Desk	24 x 7 x 365 for telephony, e-mail, and alerting (where applicable) **This explicitly includes response to P1 and P2 Incidents**		Not included

info@mti.com
www.mti.com

User Admin (Service Requests)	09:00 – 17:00 M – F excluding Bank Holidays	Not included	Not Included
Changes	09:00 – 17:00 M – F excluding Bank Holidays	Where agreed that OOH Change is required	Not Included
Incident & Major Incident Management	09:00 – 17:00 M – F excluding Bank Holidays	**P1 & P2 Incidents Only**	Not included
CyberArk Security Team Support	09:00 – 17:00 M – F excluding Bank Holidays	**P1 & P2 Incidents Only**	Not included
Service Delivery Management	09:00 – 17:00 M – F excluding Bank Holidays	Not included	Not included

4.8 Services Schedule

Full details to define the service will be mutually agreed and documented as part of the MTI CyberArk Support Service Schedule Contract prior to order, including:

4.8.1 Limitations to Service Scope

4.8.1.1 Service Accounts

The onboarding and management of service accounts within CyberArk is limited to service accounts where all discovery activities, usage patterns, and application or system dependencies have been fully identified, documented and verified by the customer (or through MTI Professional Services under separate contract) in advance. Only service accounts that can be managed using CyberArk out-of-the-box Central Password Manager (CPM) functionality, including automated password rotation, are included within scope. For any Service Account onboarded under these conditions, the customer accepts full responsibility for the identification and including of all usages and dependencies for each service account onboarded into CyberArk and takes full responsibility for any service disruption attributed to undocumented usages or dependencies breaking when the service account credentials are rotated. Any activities relating to the discovery of service accounts, identification of account usage, mapping of dependencies, remediation of hard-coded credentials, or development of custom password management workflows are explicitly out of scope. Such activities are considered custom implementation work and, where required, will be delivered via a separate Professional Services engagement or through the draw-down of Cyber Security Service Vouchers (where these have been purchased as part of the contract.)

4.8.1.2 CyberArk Version Upgrade

The PAM Managed Service includes ongoing patching and an annual upgrade of the in-situ CyberArk Vaults and CyberArk Component Server Applications running on the same underlying Server Operating Systems. In the event, the upgrade needs to be conducted on New Servers / Server OS Versions (due to software compatibility, security updates and version support), MTI will quote for additional Professional Services to migrate components and/or Vaults to the New Operating Systems.

4.8.1.3 Security (CyberArk): Standard Service Requests

Approved Service requests include:

1. Provide customer requested CyberArk documents/knowledge base articles
2. Adding / Removing Safes
3. Adding / Removing Safe Members
4. Adding / Removing Accounts

info@mti.com
www.mti.com

5. Adding accounts creating new templates
6. Mapping existing groups to CyberArk Safes
7. New mapping for groups to provide access safe
8. User Directory Role Base Access Control Mapping
9. New Directory Role Base Access Control Mapping
10. Managing CyberArk policy & password changes
11. Creating New Directory Mappings
12. Questions regarding:
    - CyberArk upgrades
    - CyberArk migration
    - Microsoft/CyberArk Patch information relating to the CyberArk Software
    - CyberArk Master Policy
    - CyberArk hardening
    - CyberArk digital vault server security standards
    - CyberArk system requirements by product/modules
    - Safes
    - Platforms
    - Vault Backup Solution queries
    - Recommendations for protecting your CyberArk deployment
    - Adding Licenses on customer environment.

4.9 Out of Scope

Below is a non-exhausted list of out-of-scope items:

1. MTI is responsible for performing only the Services described in this Proposal. All other services are considered outside of scope.
2. Any CyberArk SaaS Hosted Software solution is out of scope of support for this contract, please request the associated CyberArk Privilege Cloud / SaaS contract from MTI.
3. Any onsite working, unless agreed at additional cost.
4. Maintaining and securing the underlying servers on which the CyberArk components run is out of scope and remains the customer's responsibility.
5. If a custom connection component has been downloaded/created, this will not be covered under the CyberArk Support, however if the customer would like MTI to investigate any issues with custom connection components then a quotation can be provided, or time is drawn down form the Cyber Services Vouchers (if purchased).
6. Incidents/Services Requests (SR's) relating to: Network, Hardware, Load Balancing, 3rd Party Integrations, Active Directory, GPO's, Microsoft Patching, SSL Certificates Management, Capacity Management.
7. Incidents/SR's arising from any of the following events: Relocation, Improper operation, Fault, neglect or misuse of any Software by anyone other than CyberArk, Client's failure to maintain proper site or environmental conditions, or the failure or interruption of any electrical power, telephone or communication service or like , Any attempt at repair, maintenance, modification, new installation or upgrade to a Major Release of any Software performed by anyone other than CyberArk-certified personnel.

4.10 Customer Responsibilities

A detailed contract will be produced prior to service onboarding; however, notable customer responsibilities are below:

info@mti.com
www.mti.com

- Onboarding onto the CyberArk PAM Managed service, is conditional on the environment being in a good supportable state with no known, significant issues outstanding.
- The Managed Service includes an *Annual Upgrade* of the CyberArk platform, which MTI will deliver at a mutually agreed time. MTI's price is based on the customer providing MTI with remote access to the CyberArk applications, hosts and people required by our engineers to complete the work.
- Have a valid Manufacturer maintenance agreement with CyberArk during the MTI support period.
- Management of the Servers that the CyberArk solution resides on including but not limited to upgrading the server's operating system release.
- The Customer accepts sole responsibility for any compatibility problems between the Software and any other software, hardware, or other technology not maintained or supported by MTI/CyberArk.
- Responsible for the performance and running of server backups & restorations where CyberArk resides.

info@mti.com
www.mti.com

5 MTI Experience with CyberArk and Core PAS / PAM

MTI were the **first CyberArk partner** in the UK and have played a pivotal role in their product development and project delivery success, building a commercially and technically strong working relationship over the past 15 years. MTI has worked on multiple CyberArk deployments into various markets and has built an unprecedented working knowledge of the CyberArk Core PAS/PAM Self-Hosted solution encompassing:

- Enterprise Password Vault
- Privileged Session Manager
- Privileged Threat Analytics

Including the various components within Core PAM:

- Enterprise Password Vault (EPV)
- CyberArk - Central Policy Manager (CPM previously known as Password Manager)
- Password Vault Web Access (PVWA)
- Privileged Session Manager (PSM) for Windows, UNIX, Cloud
- Privileged Threat Analytics (PTA)
- Relevant Utilities / PrivateArk Client / Back-up Agents (PAReplicate)

And the CyberArk product extensions which may be required in the future as the deployment matures such as:

- CyberArk – Application Access Manager (AAM)
- CyberArk – Central Credential Provider (CCP)

"We consider MTI one of our top partners. MTI were the **very first CyberArk partner** in the UK. Covering all aspects of requirements gathering, to solution design, through implementation and roll out to post-sales 24/7 UK based support. As such, we do not hesitate to recommend MTI and its service capability around complex CyberArk solutions.

Head of Public Sector
CyberArk

Our experience compromises technical discovery, requirements gathering, solution design, implementation, training, roll-out and 24x7x365 UK-based support. Our support desk is staffed with CyberArk certified specialists, skilled in CyberArk technology to provide premium SLA backed support and training.

Our team are also skilled in planning and conducting Health Checks of CyberArk deployments to ensure they function and perform as expected in addition to delivering upgrades (minimising disruption to users) to ensure our customers continue to maximise their investment in CyberArk by using the latest functionality and improvements available on supported versions receiving security patches.

MTI are currently in the process of providing ongoing specialist CyberArk PAM engineering services for a multi-million-pound Central Government Department, over several years working closely with internal recourses, delivery partners and the customer's own internal teams, change processes and regulations. During this, and other similar projects, MTI have gained a vast understanding of specific processes and requirements inherent in environments with large numbers of hosts, services and users, that govern how new IT projects need to be handled and implemented and believe this unrivalled level of knowledge will be instrumental in helping The Customer implement their PAM solution in the smoothest and most reliable manner; we also offer The Customer the benefit of our PAM Project Management expertise if required.

In addition to our business / programme level experience, our technical consultants have developed templated configuration questionnaires and build documentation in addition to a library of scripts which make implementation faster, more efficient and more reliable.

info@mti.com
www.mti.com

Customer Interview - Government Department

We suspected a requirement for a Privileged Access Management (PAM) solution but did not know which flavour would fit our requirement or how it would fit within our existing complicated infrastructure or workflows. MTI assisted by evaluating our options and defining how to address our existing risk.

Without the experience of this CyberArk Platinum-accredited partner, we had little chance of successful delivery. The team shared their experience from complicated projects, including <<redacted>> which proved critical to support a successful project.

MTI suggested a number of various discovery and technological deep-dive workshops to gather the correct level of understanding of our complicated environment. That investment of time was critical to support a commercial and technical risk-free approach. With their extended resource pool of CyberArk capability and template methodology, they delivered on time and within budget.

We consider MTI to be an authority on CyberArk PAM design, implementation and support services. MTI engaged with us, advising on strategic decisions including defining a Privileged Access Policy, Role-Based Access Control and project phase definition. All consultants are extremely knowledgeable and enabled the smooth and non-intrusive rollout of the solution, whilst handing over to our main strategic ICT partner in a professional and pragmatic way.

MTI assisted with internal pre-implementation workshops and engaging with stakeholders/suppliers and end users ensuring a painless adoption. We recognised their strategic partnership with CyberArk as this came in extremely useful when looking at integration and development into third party products.

5.1 Glossary of Terms

Item	Explanation
Vault	Enterprise Password Vault (EPV)
PVWA	Password Vault Web Access
CPM	Central Policy Manager
PSM	Privileged Session Manager (Windows)
PSMP	Privileged Session Manager Proxy (UNIX)
PrivateArk Client	PrivateArk Client is the administrative interface to the Enterprise Password Vault (EPV)

5.2 MTI Internal Use

Item	Response
Presales Consultant	Kevin Foster

info@mti.com
www.mti.com

6 About MTI

MTI Technology is a technology services and solutions provider with over 200 staff, operating across EMEA with offices in the UK and Germany. Over the last 36 years, MTI has helped thousands of organisations transform their IT operations, enabling them to leverage the latest technologies, reduce operating costs, become more flexible, and mitigate risk.

MTI has considerable experience in designing, delivering, and managing cybersecurity and data centre solutions for our customers across various industry sectors, including Commercial, NHS, central government, local government, Banking, Defence, Finance, and Insurance. This extensive experience ensures your solution is designed and installed by industry-leading MTI experts, guaranteeing a smooth, accurate, and on-time project delivery.

MTI specialise in cybersecurity, data centre modernisation, IT managed services and IT transformation. By employing proven methodologies, best practices, and adopting a consultative approach, MTI helps its customers solve business challenges, providing secure and compliant management of their applications, data, infrastructure, and system environments.

6.1 Accreditations

MTI hold the following ISO Standards and Certifications

- ISO 27001 Information Security Management system
- ISO 9001 Quality Management System
- ISO 20000 IT Service Management
- ISO 45001 Occupational Health and Safety Management
- ISO 22301 Business Continuity Management System
- ISO 14001 Environmental Management System
- Cyber Essentials & Cyber Essentials Plus
- NCSC CHECK Scheme Member (CHECK 'Green Light' company since 2003)
- CREST Scheme Member

6.2 Awards

Our dedication to maintaining high standards is reflected in our numerous industry awards, including Cyber Security Customer Service Award at the Computing Security Awards 2024, Cybersecurity/Data Protection Partner of the Year Award at the CRN Awards 2024, CRN MSSP/Security Reseller of the Year 2023, CRN Security Value Added Reseller (VAR) of the year for 2018, 2019, and 2020, and Penetration Tester of the Year for 2018 and 2020. We have won the UK Service Partner of the Year award twice for excellence in service delivery, in 2023/2024. MTI is committed to delivering exceptional customer service, which is why we have an industry-leading 98% customer satisfaction rating

info@mti.com
www.mti.com

6.3 Key Platforms

MTI is proud to be recognized among the highest tier of global technology partners. This achievement underscores our leadership in cybersecurity — safeguarding critical infrastructure, protecting data across multi-cloud environments, and enabling resilience against evolving threats. Our expertise in risk management, compliance, and secure digital transformation ensures that customers can operate with confidence in today's complex, data-driven world.

Key partners include:

Microsoft Sentinel

Microsoft Defender XDR

Quest

VEEAM

BROADCOM PREMIER PARTNER VMware Reseller VMWARE DIVISION

TREND Expert

rubrik Authorised Partner

paloalto NETWORKS Innovator Partner

PURESTORAGE

CYBERARK

LevelBlue Authorised Partner

tenable

DELL Technologies TITANIUM BLACK PARTNER