

# SECURING THE ENTERPRISE'S CLOUD WORKLOADS ON MICROSOFT AZURE

# Table of Contents

Securing the Enterprise's Cloud Workloads on Microsoft Azure .....	3
Microsoft Azure and CyberArk .....	5
Using CyberArk to Secure Azure Environments .....	5
Overview .....	5
1. Securing Cloud Assets .....	7
Securing the Azure Web Portal.....	7
Monitoring and Controlling Access to Azure Instances.....	8
Implementing a Jump Server for Accessing the Azure Environment.....	9
2. Securing Hybrid Azure Environments .....	11
Securing Hybrid Environments and Other Configurations.....	11
3. Automating Provisioning Processes .....	13
Automatically Securing New Azure Virtual Machines .....	13
Summary.....	16

## Securing the Enterprise's Cloud Workloads on Microsoft Azure

Enterprises and other organizations embark on a cloud journey for a variety of reasons – some are native cloud or “all-in” cloud from the start. While an increasing number of organizations have embraced “Cloud-First” strategies, and in some cases “Automation-First” strategies, most typically operate in hybrid environments and migrate segments of their business over time to the cloud.

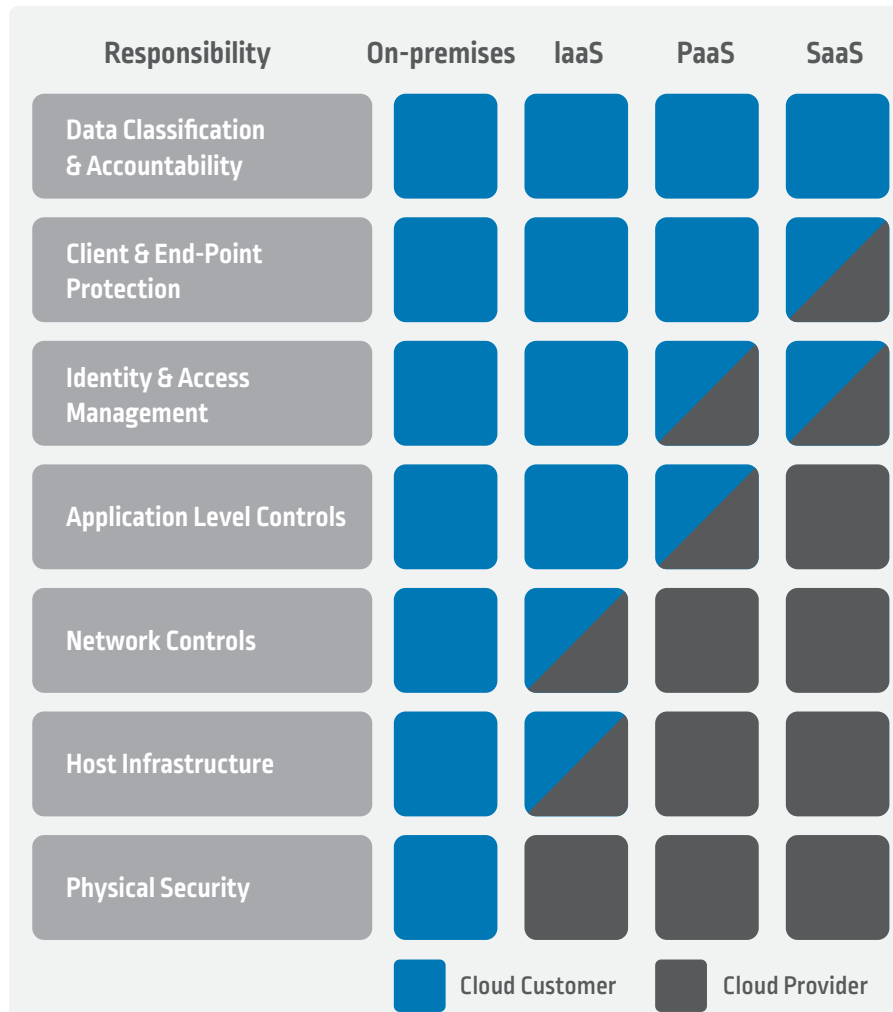
Enterprises may initially adopt cloud to support on-demand computing for applications, such as big data analytics which may intermittently require significant compute and storage resources. Organizations are also driven by cost savings, in some cases entirely eliminating the need to operate physical data centers while gaining increased efficiency. Others are driven, at least in part, by the increased availability of their applications and the overall reliability of cloud-based solutions.

Microsoft Azure (Azure) has a lot more to offer than cost savings. Enterprises with the highest levels of cloud adoption, typically, not only completely re-architect their applications, but also take advantage of automation to streamline the entire development and deployment process. They adopt DevOps pipelines and use CI/CD (continuous integration and continuous delivery) tools with the objective of nimbly meeting customer and business needs.

Regardless of where enterprises are in their cloud journey, CyberArk's goal is to enable enterprises to protect their cloud assets by providing powerful solutions for securing privileged accounts and credentials at each stage of the journey. Most important, with a CyberArk Privileged Account Security solution deployed, enterprises can consistently enforce security policies regardless of different compute environments, multiple cloud environments, delivery pipelines and automation tools.

Robust security of cloud and hybrid environments is a critical requirement for organizations. However, security in the cloud is a shared responsibility between the public cloud vendor and the enterprise. Azure and the other leading public cloud vendors go to great efforts to ensure the security OF the cloud infrastructure, including the physical infrastructure, as well as the compute, storage and networking resources. However, each of the public cloud vendors is very clear that security for IaaS (Infrastructure as a Service) and PaaS (Platform as a Services) is a shared responsibility. The enterprise, as the application owner, is responsible for protecting its data, cloud workloads, applications, client end-point protection, and at least some of the Identify and Access Management, as well as the OS and other enterprise infrastructure and assets running IN the cloud. In general for IaaS and PaaS, everything above the hypervisor or equivalent layer is the responsibility of the enterprise (refer to following diagram).

**CyberArk's goal is to enable organizations to protect their cloud assets by providing powerful solutions for securing privileged accounts and credentials at each stage of their cloud journey, including support for hybrid and mixed cloud environments.**



*Cloud Security is a Shared Responsibility – Responsibilities Vary by Cloud Service Model*  
 Source: Shared responsibilities for Cloud Computing, Microsoft Azure, V2.0 April, 2017

Additionally, organizations access their entire cloud infrastructure through the cloud vendor’s management console – for Azure this is the Azure portal. The management portal is accessed by both human users, and scripts, APIs and other non-human users.

This management portal is incredibly powerful and holds the enterprise’s “keys to the cloud kingdom,” even more so than for the on-premises admin consoles. For example, the management portal enables set up and configuration of the entire cloud infrastructure – allocating resources, setting up applications and compute instances and determining the regions that the apps run in. The portal is also used to set up all the security parameters, enabling which users have access, their level of access, and more. It also handles all the billing and is used to make purchases from the Azure Marketplace. Consequently, the management portal makes a very attractive target for attackers and must be a top priority to protect.

## Microsoft Azure and CyberArk

Microsoft Azure (Azure) is widely recognized as one of the leading providers of public cloud services, offering organizations of all sizes a highly reliable, scalable, low-cost infrastructure platform in the cloud. Azure has achieved strong growth since its launch just over five years ago with initially a PaaS and then IaaS offering. Today, Azure is broadly recognized as second in market share, and Microsoft continues to leverage its vast sales reach and ability to bundle Azure with other Microsoft products and services to drive adoption.

For customers, the Azure platform offers a broad and increasing array of capabilities and computing resources, including various compute and storage resources, including Hyper-V-virtualized multi-tenant compute (Virtual Machines) and multi-tenant storage, as well as many other IaaS and PaaS capabilities. Azure also offers one of the broadest global capabilities, including operating a worldwide network of Microsoft-managed datacenters across over 40 regions.<sup>1</sup>

In addition to internal Azure capabilities, Azure recognizes that enterprises and government organizations may seek broader solutions. Azure also supports enterprise-focused solutions from third-party vendors such as CyberArk.

Azure is an important partner for CyberArk. CyberArk's priority is to help to ensure that enterprises and other organizations can more fully secure and protect their cloud workloads running on Azure, and in Azure-oriented hybrid environments.

Today, CyberArk serves a growing group of enterprise customers using CyberArk solutions to help protect and secure their hybrid environments and cloud assets running on Azure. The configurations and customer needs can vary significantly depending upon the customers' business objectives. For example, with hybrid environments, CyberArk customers may run their primary and disaster recovery (DR) vaults in their on-premises environments, while using them to secure both Azure cloud and on-premises Microsoft environments with a single solution. In other cases, such as native cloud, customers run the primary and DR vaults on Azure.

CyberArk products running in an Azure environment are supported by CyberArk's Customer Support organization and CyberArk continues to expand its Azure-focused capabilities. Additionally, CyberArk's technical teams have developed deep expertise by working closely with enterprises, across the globe, on their Azure cloud journey - moving from evaluation, to deployment and into production. Increasingly, customers rely on the CyberArk Privileged Account Security Solution to help ensure the security of their on-premises, hybrid and "all-in" cloud Azure environments.

In summary, CyberArk works with, and offers solutions and guidance to, enterprises at each stage of their cloud journey - from evaluating security needs during an initial migration to helping ensure the enhanced security of a large enterprise wanting to extend their investments in Microsoft on-premises technology before moving to fully embrace a "Cloud-First" strategy with Azure.

<sup>1</sup><https://azure.microsoft.com/en-us/overview/what-is-azure/>

# Using CyberArk to Secure Azure Environments

## Overview

This document, comprising three sections, describes how enterprises can achieve the highest level of security for their Microsoft Azure (Azure) environments by implementing the CyberArk Privileged Account Security Solution.

1. **Securing Cloud Assets** – Describes how the CyberArk Privileged Account Security Solution helps secure Azure assets. CyberArk solutions help enterprises ensure that only authorized users are permitted to access these assets and that all access is recorded and monitored to provide a full audit trail.
  - Securing and monitoring access to the Azure Web Portal
  - Monitoring and controlling access to Azure instances
  - Implementing a Jump Server for accessing the Azure environment
2. **Securing Hybrid Environments** – Describes how the CyberArk Privileged Account Security Solution can be used to secure hybrid environments.
3. **Automating Provisioning Processes** – Describes how CyberArk Privileged Account Security solutions can help automate provisioning processes, including automatically securing new Azure Virtual machines.

# 1. Securing Cloud Assets

## Securing the Azure Web Portal

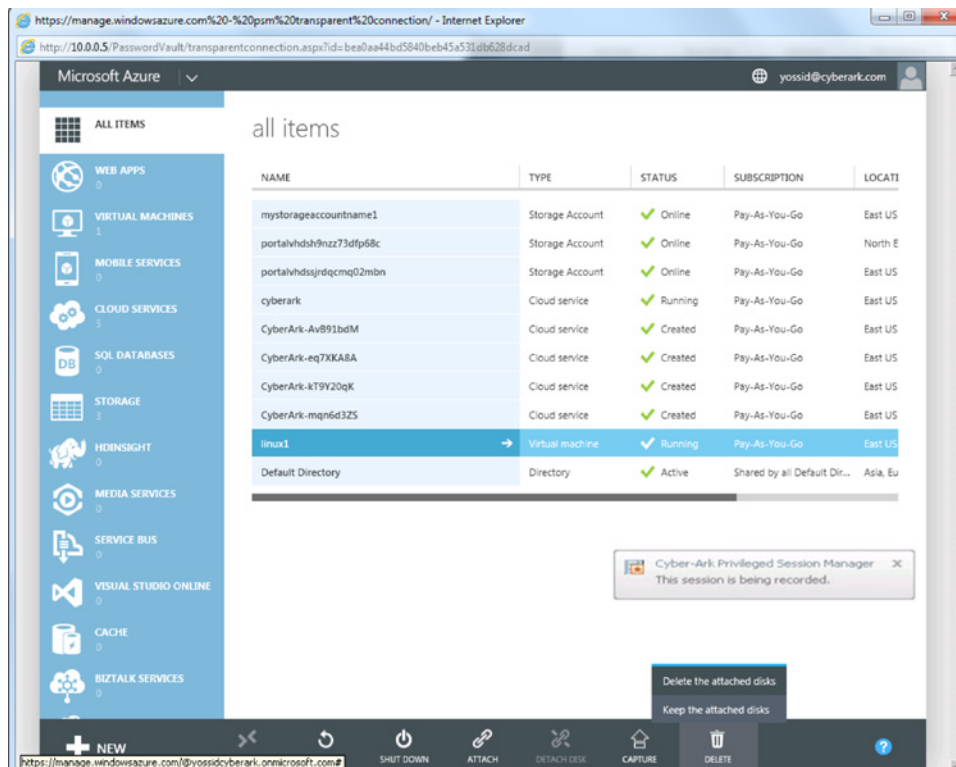
Azure administrators use the Azure Web portal or API access (e.g., PowerShell) to interactively administer the Azure cloud platform. Unauthorized or uncontrolled access to the Azure web portal directly or through APIs can lead to significant problems as the portal holds the keys to the organization’s cloud kingdom. Unfortunately, some organizations have discovered this to their peril.

Azure Active Directory is a comprehensive identity and access management cloud solution that provides a robust set of capabilities to manage users and groups and help secure access to on-premises and cloud applications including Microsoft online services such as Office 365.

An important use case is the ability to leverage CyberArk’s platform to integrate with Azure Active Directory to automatically rotate privileged users’ credentials based on an organization’s pre-defined security policy.

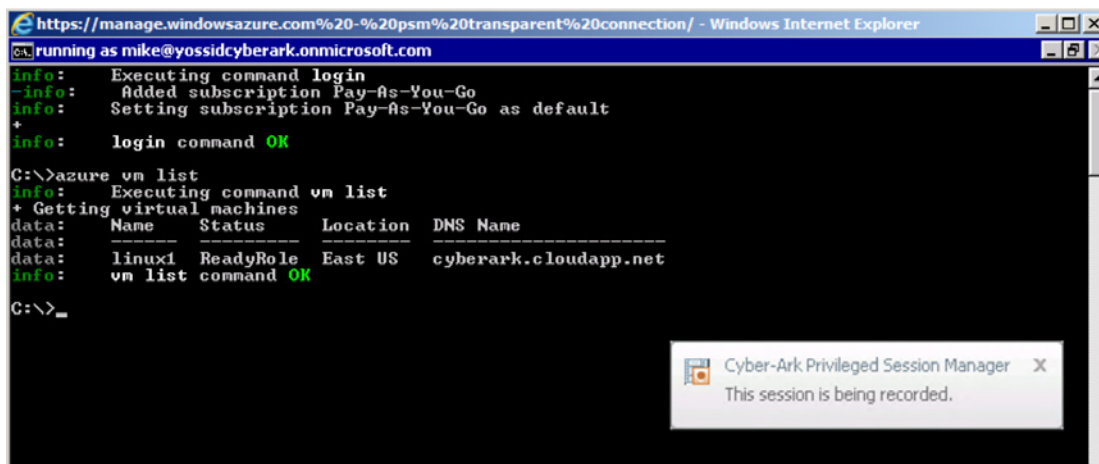
By defining Azure privileged users in the CyberArk Privileged Account Security Solution (directly or through Active Directory) and using CyberArk Privileged Session Manager to access the Azure web portal / API portals, organizations can prevent users from knowing their password to access the Azure portal. As a result, users will not be able to log in without using CyberArk Privileged Session Manager, which will audit and record everything users do during the session.

The following shows an example of a controlled session for accessing the Azure web portal.



When a maintenance activity needs to be done on Azure production instances and Azure CLI or PowerShell access is required by an IT administrator, CyberArk Privileged Session Manager will open the CLI or PowerShell console without the user seeing or knowing the Azure credentials.

The following example shows a controlled session for accessing the Azure CLI portal.



```

https://manage.windowsazure.com%20-%20psm%20transparent%20connection/ - Windows Internet Explorer
C:\>running as mike@yossidcyberark.onmicrosoft.com
info: Executing command login
- info: Added subscription Pay-As-You-Go
info: Setting subscription Pay-As-You-Go as default
+
info: login command OK
C:\>azure vm list
info: Executing command vm list
+ Getting virtual machines
data: Name Status Location DNS Name
data: -----
data: linux1 ReadyRole East US cyberark.cloudapp.net
info: vm list command OK
C:\>_
  
```

## Monitoring and Controlling Access to Azure Instances

Protecting and controlling access to Azure machines is an important security requirement. Once a privileged account credential is securely stored in the digital vault, IT administrators can access the Azure instance using CyberArk Privileged Session Manager without exposing the privileged account credentials (root, administrator, etc.) or SSH keys to the end user. This seamless access improves ease of use for administrators as well as security for the organization.

For example, CyberArk Privileged Session Manager is designed to securely obtain the privileged account password from the CyberArk Enterprise Password Vault and transparently open an RDP session to the target Windows machine while recording the full session in the background and providing detailed audit records of the user's activities. The connections secured by CyberArk Privileged Session Manager can be established through the intuitive web portal (Password Vault Web Access, PVWA) or directly from any client application or tool used for connecting to Windows servers, allowing IT administrators to maintain their standard workflows while benefiting from isolation and monitoring of the privileged activity.

The CyberArk Privileged Session Manager SSH Proxy will do the same for Linux-based machines by transparently passing the privileged account password, SSH key or any other credentials. Also, it is designed to enable end users to continue working with their native clients (e.g. Putty, SSH console) to connect to the target systems, preventing a change to the existing workflow, while maintaining the high security and audit levels.

CyberArk Privileged Session Manager helps organizations ensure that all accesses to the Azure instances are passed through the organization's security workflow (for example, a request for specific approval may be required for any access to sensitive instances). It also helps protect against credential theft by malware and keylogging techniques that can potentially infect the client machines.

Here is an example of how a user, "Mike", can initiate an SSH session to an Azure Linux machine using the CyberArk Privileged Session Manager SSH Proxy. "Mike" types the SSH command with his username, the target machine user name, target machine address, and the SSH proxy address. "Mike" will need to authenticate himself to the digital vault (which could be using his Active Directory credentials, personal SSH key, or alternatively via multi-factor authentication). In this example, once authenticated, if "Mike" has permission to access the selected Azure server, the proxy will invoke the session by transparently transferring the SSH private key to the target machine. Note, that in addition to being able to connect to the remote machine without exposing the private key, "Mike" is also monitored and recorded. Every activity "Mike" does on the target machine, including commands and keystrokes typed, will be recorded and audited. The captured audit is securely stored in the vault to help prevent "Mike" or any other user from tampering with the audit trail and destroying evidence.



```

1  [mike@localhost ~]# ssh mike@azureuser@lnx1.cloudapp.net@psmp.mycompany.com
2  mike@azureuser@lnx1.cloudapp.net@10.0.0.6's password:
3  Last login: Sun Apr  6 05:10:07 2014 from 10.0.0.7
4
5  This session is being recorded
6
7  The server's host key is not cached. You have no guarantee that the server is the computer
8  you think it is.
9  The server's rsa2 key fingerprint is:
10 ssh-rsa 2048 ee:76:92:4b:d1:f2:03:60:db:6e:8f:95:88:83:e0:45
11 If you trust this host, enter "y" to add the key to PuTTY's cache and carry on connecting.
12 If you want to carry on connecting just once, without adding the key to the cache,
13 enter "n".
14 If you do not trust this host, press Return to abandon the connection.
15
16 Store key in cache? (y/n) y
17 Using username "azureuser".
18 Last login: Sun Apr  6 08:10:28 2014 from 212.143.65.49
19 [azureuser@lnx1 ~]$
    
```

CyberArk Privileged Session Manager SSH Proxy also provides Active Directory bridging capabilities to allow users to authenticate using their Active Directory credentials (username and password) to gain access to Linux systems running on Azure. The solution enables administrators to control access to Linux systems by defining which users are permitted to log on to which systems using Active Directory. Using this system, users are logged on automatically, and users are provisioned on targeted systems when necessary. Another important capability is to de-provision users that are no longer supposed to have access to these systems. This is done automatically when users are removed from Active Directory.

## Implementing a Jump Server for Accessing the Azure Environment

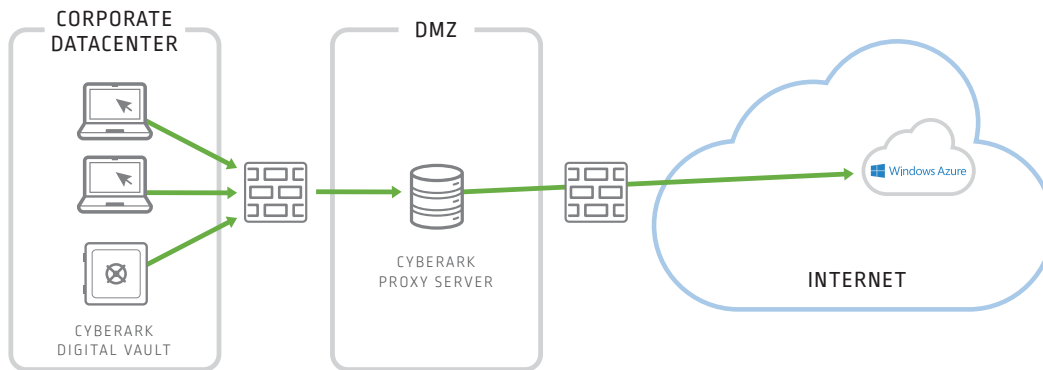
Azure Virtual Networks enables organizations to provision a logically isolated network or section of the Azure cloud to launch Azure resources in a virtual network defined by the organization. Virtual machines and services that are part of the same virtual network can access each other. However, services outside the virtual network have no way to identify or connect to services hosted within the virtual networks unless the specific connection required is configured, as in the case of VNet to VNet configurations. This provides an added layer of isolation to services running in Azure Virtual Networks. The system also enables the extension of the network into Azure and treats deployments as a natural extension to the on- premises network.

For security purposes, to reduce the size of the attack vector and secure assets on Azure, a common best practice is to limit RDP and/or SSH access to instances through a bastion host or a proxy (jump) server. The server can be located outside the organization's firewall or DMZ and used to establish a VPN connection to the Azure cloud, preventing an Azure Virtual Network connection directly into the organization's network. Any allowed access to Azure instances are only permitted from that proxy server. Also, to mitigate risks, organizations may only allow outbound communication from their environment to the Azure cloud.

CyberArk Privileged Session Manager is designed to serve as such a gateway solution, allowing organizations to achieve network segregation in a secure way and at minimal cost. The gateway is designed to be hardened and audited regularly with tamper-resistant audit logs and session monitoring for audit integrity. It can be configured to be the only access point to the cloud environment; hence firewall rules can be more restrictive and manageable since no other device/user should be accessing the cloud other than the CyberArk Privileged Session Manager Gateway.

The CyberArk Privileged Session Manager invokes a 'shadow' session to the end device to increase security. This is a different session than the one the end user is opening from their workstation. The system is designed so that any malware that the attacker is able to run on the end-user's workstation cannot propagate to the target server.

The following example shows of one possible network architecture for securing privilege sessions for the Azure environment.



CyberArk Privileged Session Manager can also be used to provide third-party contractors with secure access to the organization’s protected assets and cloud workloads. In addition to not exposing the credentials to third party users and recording the session, IT and security teams can manage the session, monitor it live and terminate it if required. Additional limitations can be implemented including limiting the time of the session, or limiting the contractor/user to a specific resource, and using a one-time password policy to change the password on the resource immediately after the session is over.

## 2. Securing Hybrid Azure Environments

### Securing Hybrid Environments and Other Configurations

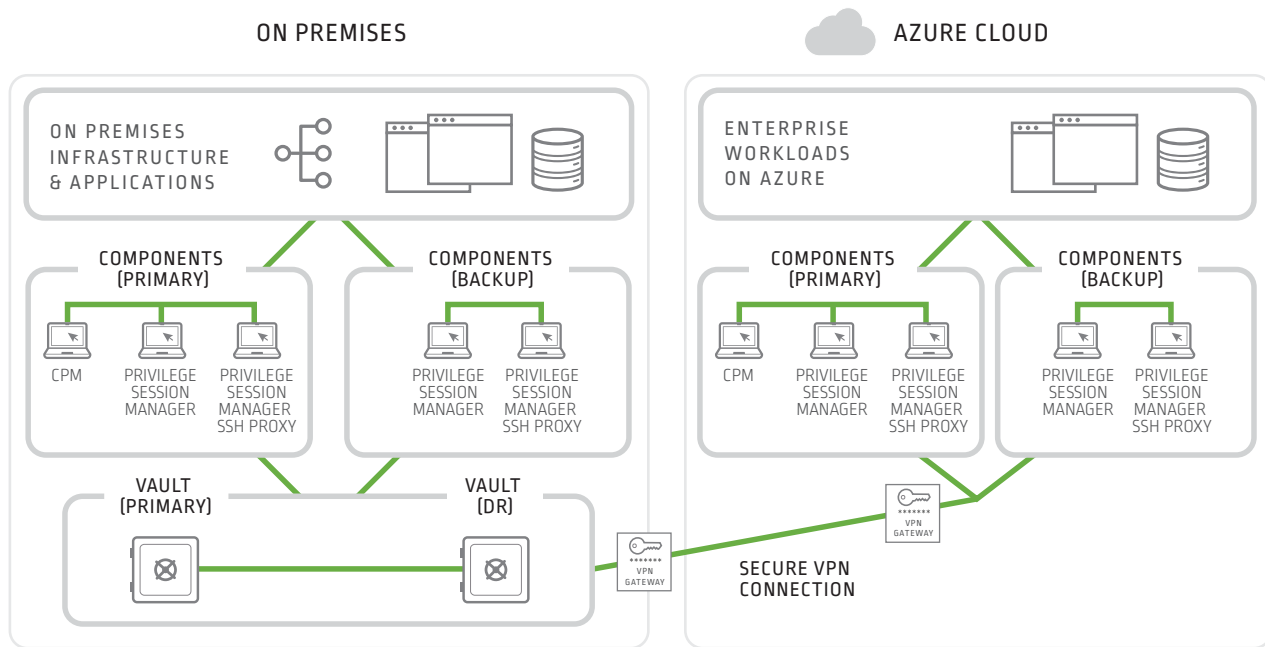
Unless organizations have fully adopted the cloud, most organizations will have some form of a hybrid environment. Enterprises migrate from on-premises to cloud environments for many reasons, including wanting the flexibility and scalability of cloud environments, elimination of data centers, and greater agility with DevOps pipelines and cloud infrastructure. Each of these scenarios may result in a hybrid environment.

Securing the operations of both the cloud and on-premises environments is one of the unique challenges of hybrid environments. This can be even more challenging when organizations use multiple cloud vendors and operate multiple on-premises environments. To consistently enforce security and access policies across hybrid environments, it is important to establish a single control point for the on-premises and cloud environment. Typically this is achieved by using the same privileged account security solution.

From architectural and performance perspective, the typical best practice (and preferred approach) is to deploy the CyberArk components; Password Vault Web Access (PVWA), Central Password Management (CPM), CyberArk Privileged Session Manager and CyberArk Privileged Session Manager SSH Proxy in the same computing environment. For optimal performance, the components must be close, from a network perspective, to the managed devices. The CyberArk architecture is designed to allow multiple instances of the components to be deployed – so components can be located on both the on-premises and Azure environments.

There are various architectural approaches for deploying the CyberArk Privileged Account Security Solution in a hybrid environment. The key decisions to make are where to deploy the primary and DR vaults, and then determine how to deploy the components to efficiently support privilege requests in the on-premises, Azure as well as possibly other computing and development environments. In organizations, with hybrid environments, that are already using a privileged account security solution, the solution will have already been deployed by the organization to help secure the on-premises environment. In this case, the primary and DR vaults will run in the on-premises data center and instances of the components will need to run in both the on-premises and hybrid environments.

A typical configuration is shown in the following diagram. Note, the diagram shows a single Azure cloud environment and a basic DR vault configuration. The CyberArk architecture is very flexible and has been configured to support complex, and demanding environments.



*Example of a Hybrid Configuration*

Note, the Vault should use a separate dedicated network to connect the CyberArk Privileged Account Security components in each of the computing environments. A secure connection, such as VPN, should be used and configured, so that the Vault can only be accessed by the CyberArk components.

Later in the organization’s cloud journey, when for example the on-premises environment is largely used for legacy applications and workloads, the primary and DR vaults can be moved to run on Azure. Of course, in “cloud first” environments, or hybrid environments that are implementing a new privileged account security solution, it may be advantageous to simply deploy the CyberArk Vault on Azure from the start.

### 3. Automating Provisioning Processes

#### Automatically Securing New Azure Virtual Machines

Automation is increasingly used to leverage the dynamic capabilities of cloud computing. For example, scripts and automation tools leveraging Azure APIs for scaling (provisioning and de-provisioning of Azure instances) are common use cases. To enable secure programmatic requests, Azure requires users to pass their credentials, so that Azure can ensure requestors have the right permission to access the requested resource. Consequently, credentials need to be assigned and secured for each new instance.

When a new instance is provisioned by Azure, whether it is a Windows or Linux machine, it includes unmanaged privileged accounts. The CyberArk Privileged Account Security Solution exposes an extensive API for storing and securing these privileged accounts in the digital vault. This API can be integrated with cloud automation/orchestration tools such as Puppet and Chef, as part of the provisioning processes, and it assures that the privileged accounts of the newly provisioned virtual machine, or container will be securely stored in the vault. The same API can be implemented to remove passwords from the vault when the instance is removed.

Another common security challenge is the risk associated with hard coded and visible credentials, including Azure Application Keys, that may be embedded in applications and scripts that utilize the Azure API. The system is designed to enable organizations to programmatically secure and make automated Azure scripts tamper-resistant by enabling scripts to run without risk of compromised Azure credentials. For example, the design enables Security Administrators to sign the applications and scripts that use the Azure critical credentials so as to help prevent anyone from being able to tamper with them. In cases when the CyberArk solution detects that a signed application was tampered with, the CyberArk solution will not provide that application with the vaulted credentials.

CyberArk offers powerful solutions designed to help ensure the security of applications. For example, CyberArk Conjur is typically used in more dynamic environments, including those leveraging DevOps tools to increase agility, and CyberArk Application Identity Manager is widely used in less dynamic environments. Both can scale extensively.

The following is an example of a PowerShell script that programmatically provisions a new Windows machine on Azure infrastructure, automatically stores the account credentials in the digital vault using RESTful API calls and starts managing the administrator account based on the organization’s security policy. Similar code can be used in a Puppet module, Chef recipe, or other similar automation tools.

```

1      #####
2      #get Azure user name and password from the Vault
3      #Note: Any changes to the script done after the script has been signed to the Vault will cause this call to fail.
4      $AzureCred = C:\CyberArk\ApplicationPasswordSdk\CLIPasswordSDK.exe GetPassword /p AppDescs,
5      AppId="AzureConnect" /p Query="Safe=Azure;Object=Azure API Access" /o "PassProps.userName,Password"
6      #####
7      if ($AzureCred -eq $null){
8          Write-Host "Failed to get Azure credentials from the Vault"
9      }
10     else {
11         # Get the API login password from CyberArk Vault using CyberArk AIM.
12         $CALoginPass = C:\CyberArk\ApplicationPasswordSdk\CLIPasswordSDK.exe GetPassword /p
13         AppDescs.AppId="AzureConnect" /p Query="Safe=Azure;Object=api_pwd" /o "Password"

```

```

13      #Azure authentication
14      $pos = $AzureCred.IndexOf(",")
15      $AzureUserName = $AzureCred.Substring(0, $pos)
16      $AzurePwd = $AzureCred.Substring($pos+1)
17
18      $securePassword = ConvertTo-SecureString -String "$AzurePwd" -AsPlainText -Force
19      $cred = New-Object System.Management.Automation.PSCredential($AzureUserName,
$securePassword)
20      Add-AzureAccount -Credential $cred
21
22      #####
23      #Create new Instance
24      Set-AzureSubscription -SubscriptionName "Pay-As-You-Go" -CurrentStorageAccount
"portalvhdssjrdqcmqO2mbn"
25      $vmid = "s01"
26      $VMName = "MyVM-" + $vmid
27      $ServiceName = "CyberArk-" + $vmid
28      $AdminUsername = "cyberark"
29      $VMImageName = "bd507d3a70934695bc2128e3e5a255ba__RightImage-Windows-2012R2-
x64-v14.2"
30
31      #generate random strong password for the administrator user
32      C:\CyberArk\Pacli\pacli INIT sessionid=1
33      $Password = C:\CyberArk\Pacli\pacli GENERATEPASSWORD LENGTH=8 MINUPPERCASE=2
MINSPECIAL=-1 MINLOWERCASE=2 MINDIGIT=2 sessionid=1
34      C:\CyberArk\Pacli\pacli TERM sessionid=1
35      $Windows = $true
36      $VMInstanceSize = "ExtraSmall"
37      $WaitForBoot = $true
38      "Creating $VMName..."
39      New-AzureService -ServiceName $ServiceName -Location "East US"
40      $AzureVM = New-AzureQuickVM -ServiceName $ServiceName -ImageName $VMImageName
-AdminUsername $AdminUsername -Password $Password -Windows:$Windows -InstanceSize
$VMInstanceSize -Name $VMName -WaitForBoot:$WaitForBoot
41      "Get VM and set RemoteDesktop and Secure PowerShell endpoint..."
42      $vm = get-AzureVM -Service $ServiceName -Name $VMName
43      $vm | Set-AzureEndpoint -Name "RemoteDesktop" -PublicPort 3389 -LocalPort 3389 -Protocol
"tcp" | Update-AzureVM
44      $vm | Set-AzureEndpoint -Name "PowerShell" -PublicPort 5986 -LocalPort 5986 -Protocol "tcp" |
Update-AzureVM
45
46      $DNSName = $ServiceName + "." + "cloudapp.net"
47      $loginURI = "http://10.0.0.5/PasswordVault/WebServices/auth/cyberark/
CyberArkAuthenticationService.svc/logon"
    
```

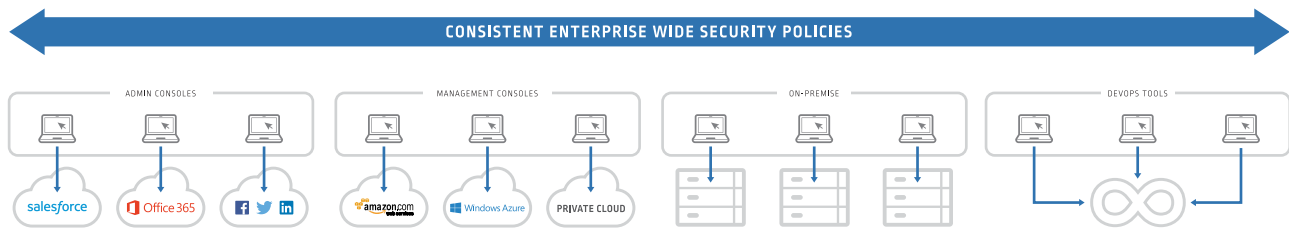
```

48         $logoffURI = "http://10.0.0.5/PasswordVault/WebServices/auth/cyberark/
CyberArkAuthenticationService.svc/logoff"
49         $createAccountURI = "http://10.0.0.5/PasswordVault/WebServices/PIMServices.svc/Account"
50         $loginInfo = @{}
51         $loginInfo.username = "api"
52         $loginInfo.password = $CALoginPass
53
54         # account parameters
55         $newAccounts = @{}
56         $newAccount = @{}
57         $newAccount.safe = "Azure"
58         $newAccount.platformID = "WindowsPowerShell"
59         $newAccount.address = $DNSName
60         $newAccount.username = $AdminUsername
61         $newAccount.password = $Password
62         $newAccount.accountName = $VMName + "-" + $AdminUsername
63
64         $newAccounts.account = $newAccount
65     # login to the Vault
66     $result = Invoke-RestMethod -Method Post -Uri $loginURI -ContentType "application/json" -Body
(ConvertTo-Json($loginInfo))
67     $logonToken = $result.CyberArkLogonResult
68     "Vault login successfully"
69     $headers = @{ "Authorization" = $logonToken }
70     # create the account in the Vault
71     $result = Invoke-RestMethod -Method Post -Uri $createAccountURI -headers $headers -ContentType
"application/json" -Body (ConvertTo-Json($newAccounts))
72     # logoff from the Vault
73     $result = Invoke-RestMethod -Method Post -Uri $logoffURI -headers $headers -ContentType
"application/json" -Body (ConvertTo-Json($loginInfo))
74     "Vault logoff successfully"
75     "finish creating account $VMName-$AdminUsername-$DNSName"
76     }
    
```

## Summary

CyberArk enables enterprises to protect their cloud assets by providing powerful solutions for securing privileged accounts and credentials at each stage of the cloud journey.

An increasing number of organizations don't use just one cloud provider, but for various reasons use multiple cloud providers - business flexibility, multiple business lines, prior acquisitions, geographic coverage, redundancy, etc. Additionally, enterprises often have legacy, on-premises and hybrid environments, in which case, the same IT administrators may access and manage multiple compute, development and automation environments. CISOs and IT leaders want, as a best practice, to be able to enforce the same security and access policies across the entire enterprise regardless of the compute environments, delivery pipelines and automation tools.



*Single Control Point Enables Consistent Enforcement of Security Policies*

To implement this best practice, enterprises typically want to manage privileged user credentials and access permissions with a digital vault as a single control point.

CyberArk provides solutions for Azure and other cloud providers, including AWS and Google. In response to strong customer demand, CyberArk continues to enhance and expand its cloud and DevOps capabilities to meet the evolving needs of organizations adopting the cloud.

Whether your organization has fully embraced the cloud or is just starting the journey, it is essential to implement robust privilege management policies to protect your cloud assets. CyberArk has the solutions, resources and cloud expertise to help enterprises protect and secure the “keys to their cloud kingdom”.

For additional information visit [cyberark.com/cloud](https://cyberark.com/cloud).

©Copyright 1999-2017 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 11.2017. Doc # 171

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.