# Secure and Scalable Management with Arcible Vision

{$_. arcible }

This document is issued by Arcible Limited. Arcible makes no warranties, expressed or implied, in this document.

Compliance with copyright laws is the responsibility of the user. No part of this document is to be reproduced, stored or introduced into a retrieval system or transmitted in any form or by any means, for any purpose, without the express written permission of Arcible.

This document is version controlled and maintained electronically by Arcible. Any printed or externally issued copies of this document are not subject to version control and may be out-of-date. It is the responsibility of the user to ensure that they are working with the latest version of the document.

The descriptions of other companies' products in this document, if any, are provided as a convenience. Any such references should not be considered an endorsement or support by Arcible. Arcible cannot guarantee the accuracy of this document as products may change over time. Descriptions are intended as brief highlights to aid understanding and are not comprehensive product details. For authoritative descriptions, please refer to the respective product manufacturers.

# Table of contents

# Introduction

When you are working with a partner, you want one that understands your operation and one that works with the products and services you use and for us, that's Microsoft Azure. Arcible Vision is our light managed services offering. Powered by Azure Lighthouse, Arcible Vision provides us with the capability to securely and seamlessly help you to manage your Azure workloads.

In this guide to secure and scalable management with Arcible Vision and Azure Lighthouse, we walk you through how the onboarding process works, some typical scenarios we can use Azure Lighthouse for, and information about security of the solution.

Every customer is unique and while we've done our best to answer common questions and scenarios in this guide, nothing beats a conversation.

If you are interested in management of your Microsoft Azure Subscriptions. Azure Lighthouse, and Arcible Vision, then get in touch with us to speak to us and find out more. You can email us at info@arcible.com to get started.

# How Azure Lighthouse works

Unlike traditional management approaches where you would create numerous accounts in your own environment for users at your partner organisation, with Azure Lighthouse you create none.

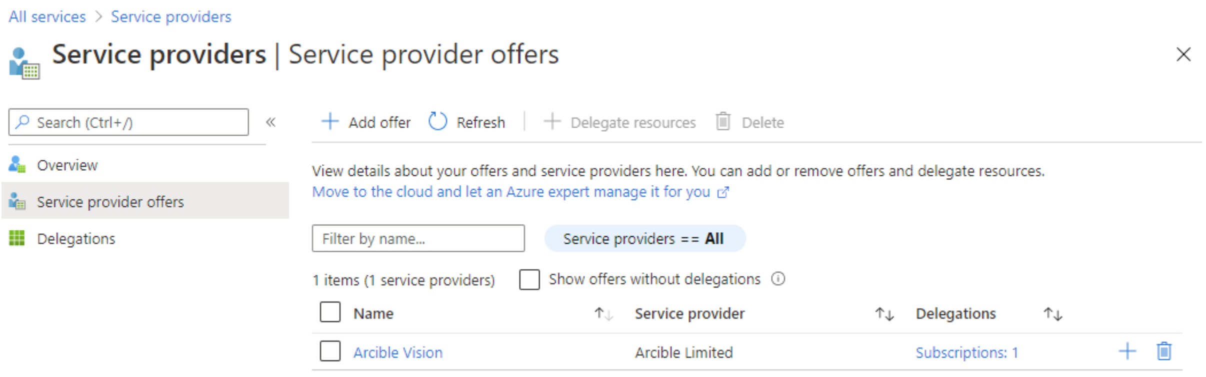
To get set-up you complete a simple, guided onboarding process and we take care of the rest.

Azure Lighthouse works by delegating permission to users in the Arcible Service Provider environment to the Azure Subscriptions you request. So what are the benefits of this approach to you?

- No overhead to provide on-going management of partner accounts and identities
- No licensing cost to you to provide access for management purposes
- No need to embed Arcible into your processes and policies such as a joiners and leavers process or enforcement of password policy
- No worries about over-provision of access

Azure Lighthouse overcomes these common issues by giving you a kill switch that you can simply operate when you want to terminate the delegation.

Azure Lighthouse uses the Azure Role Based Access Control (RBAC) permissions model. As a delegated partner, we never have Owner permissions to your resources; the highest role we can ever have is Contributor.



All services > Service providers

Service providers | Service provider offers

View details about your offers and service providers here. You can add or remove offers and delegate resources.
Move to the cloud and let an Azure expert manage it for you

Filter by name...

Service providers == **All**

1 items (1 service providers) □ Show offers without delegations

| □ Name | Service provider | Delegations |
|---|---|---|
| □ Arcible Vision | Arcible Limited | Subscriptions: 1 |

Figure 1: Our Arcible Vision Service Provider offer can be removed with a single click giving you a kill switch to remove our access anytime

If you want to limit what resources we have access to, no problems. Azure RBAC allows us to be granular and specify specific Resource Groups where we do and don't have a delegation. Maybe you want to give Arcible read-only access to one Subscription for oversight and Contributor to another for management? Again, no problem.

# Typical management scenarios

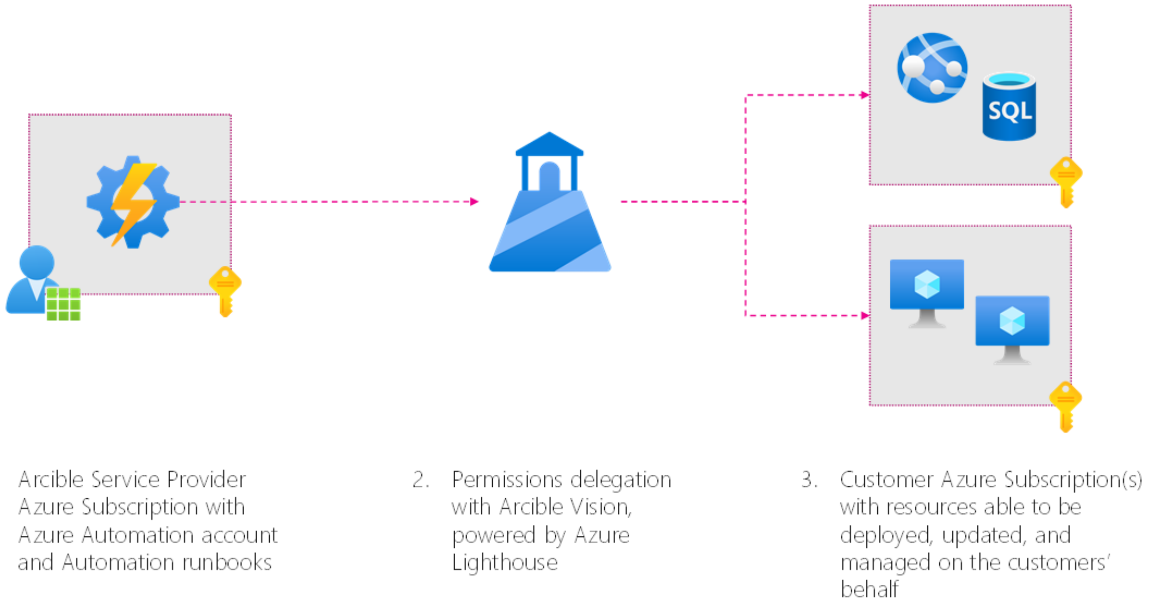
With Arcible Vision, there are two management scenarios that we commonly think about.

- Management of resources and workloads
- Aggregate reporting and oversight

## Management of resources and workloads

You may have one Subscription in Microsoft Azure or you may have many. In either case, trivial or repetitive tasks are both time consuming and prone to human error when implemented manually. Even with automation, if you have multiple Subscriptions, costs can add up when you implement a solution repeatedly across them.

With Arcible Vision, powered by Azure Lighthouse, Arcible has delegated permission to deploy, update, and manage resources and workloads in your Microsoft Azure Subscription.



1. Arcible Service Provider Azure Subscription with Azure Automation account and Automation runbooks
2. Permissions delegation with Arcible Vision, powered by Azure Lighthouse
3. Customer Azure Subscription(s) with resources able to be deployed, updated, and managed on the customers' behalf

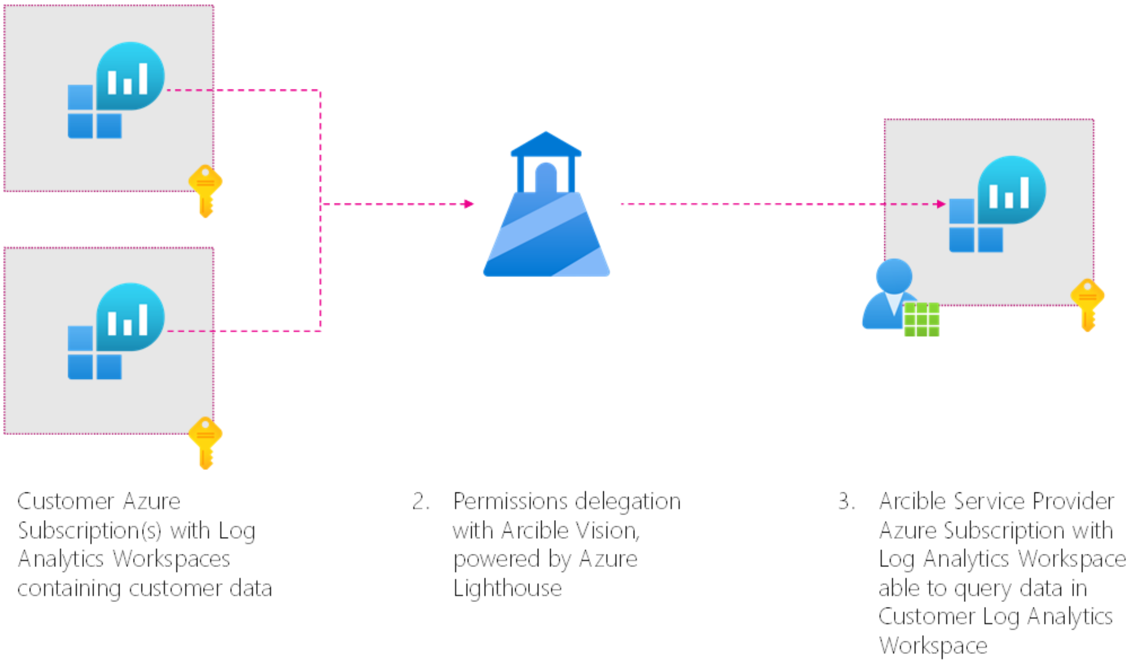
Figure 2: With centralised, scalable management, Arcible can centrally deploy, update, and manage your Microsoft Azure workloads across multiple Subscriptions

Using the capabilities provided by Azure Lighthouse, we can centralise and consolidate management activities for you from our Service Provider environment. Using tools like Azure Automation, we can reliably and repeatably deliver the results you need. Because the relationship is one-to-many, we can manage any number of Azure environments for you from a single pane.

## Aggregate reporting and oversight

Once you have deployed workloads in Microsoft Azure, you want and need to keep on top of them. Maybe you are using Azure Update Management as a cloud-based patch management solution for your systems and need a way to centrally see multiple Azure Subscriptions and the state of play across them all.

With Arcible Vision and Azure Lighthouse, Arcible can read data from your Log Analytics Workspaces back to a single, central, Log Analytics Workspace in our Service Provider environment. From here, we can aggregate data from multiple Subscriptions to give you a single view of the estate making it as scalable as you need it to be.



1. Customer Azure Subscription(s) with Log Analytics Workspaces containing customer data
2. Permissions delegation with Arcible Vision, powered by Azure Lighthouse
3. Arcible Service Provider Azure Subscription with Log Analytics Workspace able to query data in Customer Log Analytics Workspace

Figure 3: By reading data with our Arcible Service Provider environment, we can report and provide oversight on your Microsoft Azure resources regardless of how diverse they are

Arcible never owns the data: you do. As Service Providers, we have no accounts within your own environment as access is delegated to us not given to us.

Using solutions like Azure Update Management, Log Analytics Workspaces are in your own Subscriptions and your own region of choice are used.

# Azure Lighthouse and security

When we're talking about your businesses data, you want to know that it's safe and in safe hands. You also want to know that you are in control of it. Arcible Vision and Azure Lighthouse are designed with exactly these concerns in mind.

When you onboard into Arcible Vision, you call the shots picking where you want us to have access. If our off-the-shelf onboarding script does not meet your needs, then we can work with you to customise the onboarding experience for the level of access you want to delegate.

## Your data, your control

Once onboarded, you remain in complete control. Everything in Microsoft Azure remains in your Subscriptions under your control, in the Azure datacentre locations and regions that you want.

When we deploy resources for you, the product is all yours and not hosted by us or owned by us. When we provide reporting or oversight into services you use, we're just reading the data you have not keeping it for ourselves.

If you decide that it's time to move on and no longer wish to use Arcible Vision, simply remove us from the Service Providers offerings in your Microsoft Azure Portal and all our access goes away at once. No need to worry about what accounts we had or anything else.

## Our security, your trust

Users at Arcible can only gain access to customer environments once they have been granted access to do so and we strictly manage who gets that access. We break-down access rights into two tiers of support for read-only users and users with the ability to perform management of resources to even further limit access.

Arcible users are subject to strict controls and restrictions limiting when, where, and how we can sign-in so that you can be confident in the access you give us.

Arcible users accessing customer environments through Azure Lighthouse only ever do so from within the UK; multi-factor authentication is required for all access to Microsoft Azure at Arcible.

We perform automated audits of access and remove users that no longer require access. Our default response is remove access so that access doesn't linger for any reason.