Cloud Insights

Proof of Value

Gain visibility and innovate faster with insights across your hybrid infrastructure

With Cloud Insights, you can **protect** your data, monitor, troubleshoot and **optimise** all your resources in your private data centres and public clouds.

Proof of Value

Sometimes seeing is believing. All too often vendors, service providers & consulting firms such as ourselves spend an inordinate amount of time preparing presentations, business cases, ROI calculations, white papers and technical validation reports etc. We host meeting after meeting, often over weeks or months, frankly, wasting your time and ours. While we have done case studies and can provide white papers, we believe there is a better way…

Our Hybrid Cloud Insights Proof of Value (POV) provides real-time, live analytics across the selected environment. Diverse dashboards are available to suit various business and technical functions. These dashboards provide a visualisation of the topology, availability, performance and utilisation of your public cloud and on-premise multi-vendor resources.

Of immediate value is the identification of unused or abandoned resources – providing you the opportunity to right-size your environment and optimise your spend with your cloud and/or on premise vendors.

At the conclusion of the POV, all data and metadata collected will be deleted unless otherwise requested by you.

Security of Your Data & Business Intellectual Property (IP)

Confidentiality: We take our relationship with you and your business seriously. If requested, we will execute a Mutual Non-Disclosure Agree (NDA) or Confidentiality Agreement. We will not disclose information provided to us during the Proof of Value. You may use our standard Mutual NDA or your own (please select & tick your preferred option on the following page).

Security: Our Cloud Insights software follows security best practices throughout the release life cycle to make sure your information and data is secured in the best possible way. Security, processes, and services are subject to independent third-party audit and validations from an externally licensed CPA firm, including completion of a SOC 2 Audit.

For more detailed information on the security of the product and your customer data you can download our Cloud Insights Security Overview document.

(https://diversusgroup.com/dg-cloud-insights-security-overview/)

Cloud Insights
Proof of Value

Top 3 Business Benefits of Cloud Insights

1. Reduce mean time to resolution by 90% and prevent 80% of cloud issues from impacting end users
2. Reduce cloud infrastructure costs by an average of 33%
3. Reduce your exposure to insider threats by protecting your data with actionable intelligence

Preparing for the POV – What is Required?

In order to run the POV with you we need to deploy a data collector within your relevant cloud service.

Cloud Environment: Please advise which public cloud environment you would like to analyse during the POV:

- ☐ Amazon Web Services (AWS)
- ☐ Microsoft Azure
- ☐ Google Cloud Platform (GCP)

NDA

Would you like to execute a Non-Disclosure or Confidentiality Agreement in advance of the POV?

- ☐ Yes
- ☐ No

If yes, please indicate if you would like DG to provide a completed mutual NDA or if you will provide:

- ☐ DG Mutual NDA format
- ☐ Your format

Data Collector Requirements – the Technical Bit…

A member of your IT team will need to work with one of our technical consultants to prepare and deploy the relevant data collector. Generally, an investment of no more than 1-2 hours is required.

The technical requirements for Azure, AWS and GCP are detailed below:

Microsoft Azure

- ☐ Port requirement: 443 HTTPS
- ☐ Azure Management Rest IP (management.azure.com)
- ☐ Azure service principal client ID (user account)
- ☐ Azure service principal authentication key (user password)
- ☐ You need to set up an Azure account for Cloud Insights discovery.

Once the account is properly configured and the application is registered in Azure, we will have the credentials required to discover the Azure instance.

The following link describes how to set up the account for discovery: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Amazon Web Services (AWS)

- ☐ AWS EC2 Devices:
- ☐ Port 433 HTTPS
- ☐ IAM Access Key ID
- ☐ Secret Access Key for your Amazon EC2 cloud account
- ☐ "list organization" privilege

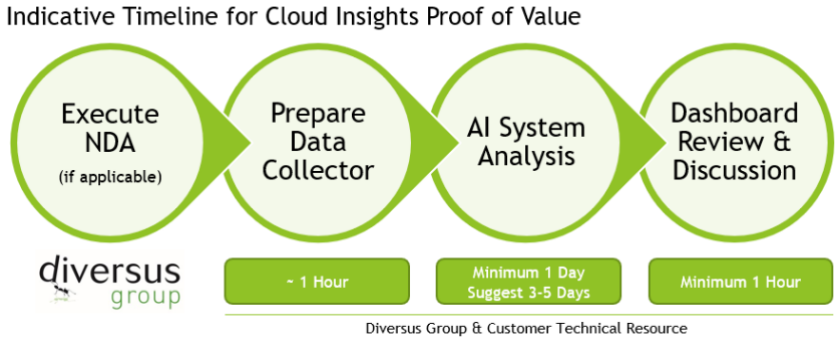
EC2 Instances can be reported as a Virtual Machine, or (less naturally) as a Host.

EBS Volumes can be reported as both a VirtualDisk used by the VM, as well as a DataStore providing the Capacity for the VirtualDisk. Access keys consist of an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). You use access keys to sign programmatic requests that you make to EC2 if you use the Amazon EC2 SDKs, REST, or Query API operations. These keys are provided with your contract from Amazon.

Google Cloud Platform (GCP)

- Project ID for the Google Cloud Platform configuration
- Client ID for the Google Cloud Platform configuration
- Your Google credentials for the Cloud Platform account

Indicative POV Timeline



In terms of expectation management, we suggest an elapsed duration of 5 business days (to allow sufficient data insights to be developed). Allow 1-2 hours for a technical resource to work with us to establish the environment & 2-4 hours per attendee for the subsequent review and discussion meeting.

Contact Us

For more information, contact your DG Account Manager.
contactus@diversusgroup.com
www.diversusgroup.com