



delaware

Connecting SAP RISE through Connectivity HUB

February - 2022



 delaware

“Average total cost of a data breach is
**\$3.86 million, nearly 40% from lost
business**”

source: [Cost of a Data Breach Report 2020 - Ponemon Institute/IBM](#)



ERP systems contain vast amounts of **confidential and sensitive data that** must be accessed in a controlled and monitored schema.

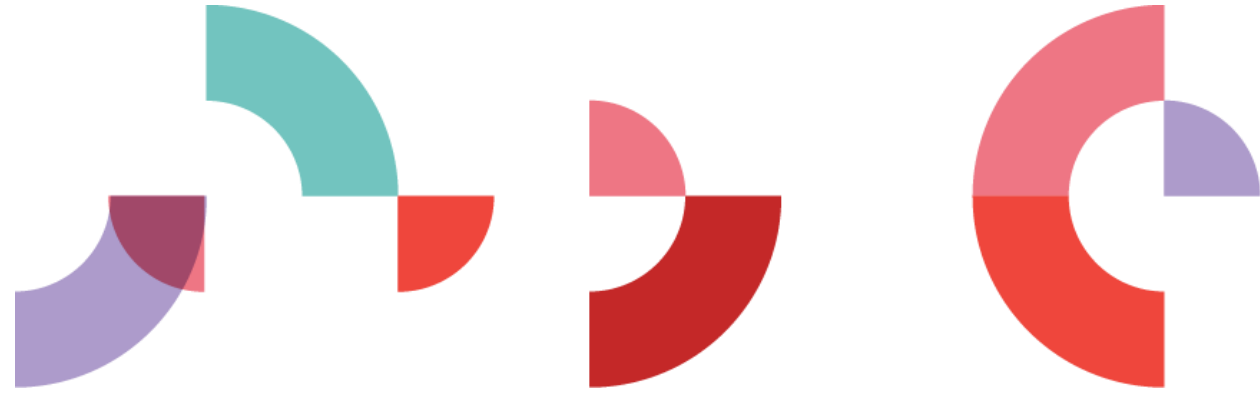


As an SAP technology partner with a wide background of executed projects, **delaware** has been part of implementations where has supported its clients to:

Solve and improve communication problems towards SAP

Evaluate scenarios where latency can be so high that affects the productivity of the environment

Improve environments in which long times are required to obtain extra connectivity, avoiding the effects of a connection without the minimum standard.



But, how can **delaware** support your organization in this process?

Providing best practices on a Connectivity HUB:

- VNET peering to SAP RISE with full connectivity from RFC-1918
- Connection to the HUB based on Microsoft PaaS components or NVA
- Possible additional services with AVD

In **delaware** we support our customers with the proper design of a segmented and secure infrastructure capable of isolating important SAP workloads hosted in Microsoft Azure



“SAP offers connectivity towards SAP RISE, based on:
Public Access
Virtual Private Networks
ExpressRoute
VNET Peering (only within Microsoft Azure)”

But, do you really understand
why the **connectivity HUB** model
is what your organization
requires?

some technical reasons

connecting SAP RISE through Connectivity HUB

The efficiency of SAP is based on many aspects, but one of them is the correct use of the best practices of the environments and periodic updating necessary due to global innovations, which requires a controlled exposure and turns these resources into a focus of attention for possible data leaks.



connecting SAP RISE through Connectivity HUB

why connect our workloads through HUB architectures?

the HUB spoke principle in Azure to control SAP workloads, it divides everything into separate workspaces where we can set-up properly access based on the business/IT needs.

The common elements to use are the hub and spoke arc to isolate traffic from other virtual networks.



connecting SAP RISE through Connectivity HUB

why connect our workloads through HUB architectures?

- VNet peering to SAP RISE securely connects Azure resources to other entities.
- Using this architecture, a virtual network connects to an on-premises environment through a gateway deployed at the center of a hub-and-spoke topology.
- The spoke is the virtual network used for the SAP services.



delaware, has been part of SAP projects where is in place the Azure virtual data center architecture to communicate using a hub-and-spoke model, providing a central point of connectivity where Azure Firewall and other types of Network Virtual Appliances (NVAs) could be deployed to inspect and control traffic routing where your SAP systems reside.



we commit. we deliver.