Customer Story: Scalable Global Routing for Hybrid Cloud in the Insurance Industry



BLUECAT™



Employees: 37,000+

Revenue: $40B

Business footprint: Global

Industry: Insurance

Architecture:
12 data centers (consolidation in progress), eight Microsoft Azure regions (expansion in progress), and small pockets of Amazon Web Services (AWS) and Google Cloud Platform (GCP)

The challenge: Cloud expansion hits a snag

"We really leaned into Azure five years ago," says this multinational insurer's AVP of Global Network Services. "Now, all applications that we're newly developing, or substantially modernizing, need to go to Azure. If not, there has to be a good reason."

With approximately 20 application sites and more than 450 user sites to interconnect, this insurer wanted to continue seamless operations. More importantly, it wanted consistent policy enforcement, security, and risk management across its entire hybrid estate.

"Security is priority number one here," the insurer's technology leader elaborates. "Naturally, our two biggest goals were to standardize visibility across our hybrid estate, and consistently be able to lock things down." So, the security and risk team mandated the use of private IP for internal network resources.

To satisfy this requirement, the cloud team deployed Private Endpoints in Azure to secure the IP without much understanding of the networking implications. Unfortunately, this made it impossible to resolve DNS (and therefore ensure connectivity) between data center resources and Azure DNS zones.

The cloud team realized they couldn't satisfy both their security and scalability requirements using their Azure toolset alone.

The solve: Existing on-premises resources offer a viable, less expensive solution

To find a viable solution, the cloud team put their heads together with their counterparts in networking. They also consulted the network team's on-premises DNS, DHCP, and IP address management (together known as DDI) vendor, BlueCat. The resulting solution, which is in production today, satisfies all the insurer's requirements and then some.

Combining the wealth of knowledge, experience, and tools from both cloud and network teams, the insurer managed to:

- Reduce global operational costs due to a consolidated management platform and automation;
- Improve its security and compliance posture through global visibility in addition to the support of private IP; and
- Shorten time to deploy services in its hundreds of Azure subscriptions.

The lesson learned: Involve your networking team and vendors

Eighty-eight percent of cloud and networking professionals agree that the network team should have visibility and input into hybrid cloud design, and for good reason. For this multinational insurer, enabling security and interconnectivity across their global hybrid estate wouldn't have been possible without input from networking.

Along the way, BlueCat's DDI experts worked closely with this organization's cloud and networking technologists to propose architecture and technology solutions that allowed them to achieve their goals.

Canada Headquarters

4100 Yonge St. 3rd Floor
Toronto, ON M2P 2B5
Canada

1-866-895-6931

USA Headquarters

156 W. 56th Street, 3rd Floor
New York, New York 10019
United States

1-866-895-6931

© 2020 BlueCat Networks (USA) Inc. and/or its affiliates. All rights reserved. BlueCat, BlueCat Networks, the BlueCat logo, BlueCat DNS/DHCP Server, BlueCat Automation Manager, BlueCat Address Manager, BlueCat Device Registration Portal and BlueCat Threat Protection are trademarks of BlueCat Networks (USA) Inc. and/or its affiliates. All other product and company names are trademarks or registered trademarks of their respective holders. BlueCat assumes no responsibility for any inaccuracies in this document. BlueCat reserves the right to change, modify, transfer or otherwise revise this publication without notice.

Accessible Document