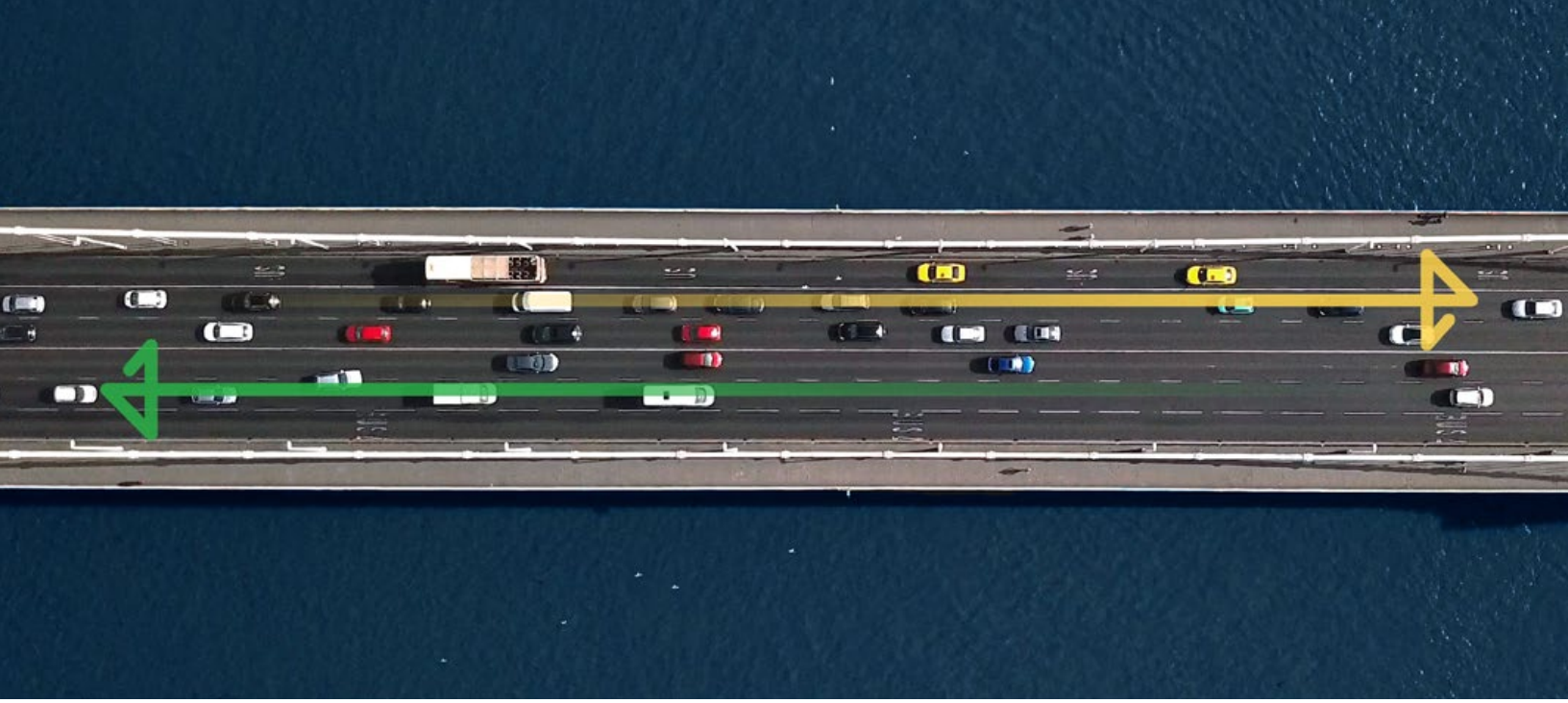
Migration Case Study – Federal System Integrator

BLUECAT™



The Customer

In April 2018, an acquisition created one of the largest Federally-focused system integrators. In the aftermath of that deal, the combined entity decided to sell off part of its business to a leading provider of call center solutions. The buyer of the call center business was one of the largest service providers to Federal agencies, including the Centers for Disease Control, the IRS, the Department of Veterans Affairs, and the Social Security Administration.

The Challenge

The acquisition presented a significant logistical challenge for network administrators at both the new Federal system integrator and the call center company.

The window for closing the deal was tight – just four months. During that time, the Federal system integrator needed to identify all of its assets associated with its call center business, extricate them from its existing network infrastructure, and deliver them to the call center solution provider.

Modern call centers all use IP-enabled phones, making IP address allocation a critical part of service delivery. This technology choice produced the requirement that the existing network be delivered to the call center provider with zero downtime. Given the 24/7 nature of the call center business and the strict SLAs of clients on both sides of the acquisition, no scheduled maintenance windows were available to make the transition.

The Solution

The Federal system integrator engaged BlueCat, its DNS provider, to split off the DNS resources associated with its call center business and deliver them to the call center provider.

To meet the strict requirements for no downtime and no maintenance windows, the BlueCat team decided to pursue a strategy of parallel deployments which would shift from one company to another over time.

To start, the BlueCat team worked with the Federal system integrator to identify and isolate the assets within their network which were in scope for the migration. This involved splitting the customer instance for BlueCat's DNS Integrity platform and concentrating all acquisition-related assets in one zone.

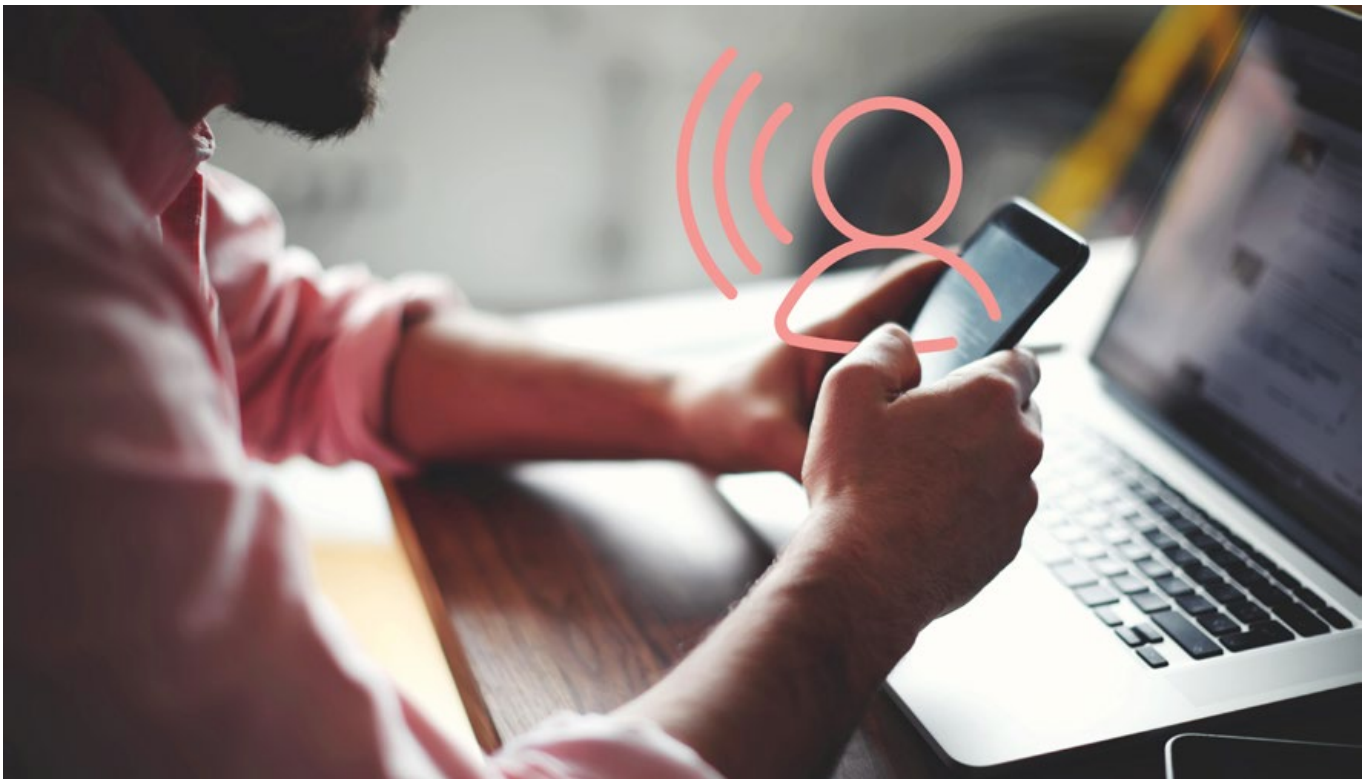
The BlueCat team also stood up an instance of DNS Integrity for the call center provider, working with the network team to seamlessly integrate it into the existing hodgepodge of Microsoft, Infoblox, and other DNS management solutions.

Over the course of the transition period, BlueCat gradually cut over assets zone by zone from one company to another according to a strict timetable. After each DNS zone was tested and operational on the call center provider's network, BlueCat spun down the parallel zone on the Federal system integrator's system.

The Result

BlueCat delivered a fully functional DNS management system within the acquisition timeframe, all with zero downtime or scheduled maintenance windows. The call centers were fully operational on both sides of the acquisition as assets were migrated in the background over the course of four months.

Even as they set out the statement of work, project managers from both companies were skeptical that such a complicated migration could be delivered within the scheduled window, let alone with no downtime involved. Through close collaboration with network administrators on both sides and the use of its proprietary migration technologies, BlueCat was able to exceed customer expectations.



Canada Headquarters

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

1-866-895-6931

USA Headquarters

1000 Texan Trail, Suite #105
Grapevine, Texas
76051
United States

1-866-895-6931

BLUECAT™

Customer Story: Scalable Automation Initiatives in the Healthcare Industry

BLUECAT™

Employees: 129,000

Revenue: $18B

Business footprint: USA

Industry: Healthcare

Architecture:
Two data centers with local servers at each of about 50 sites

The challenge: Their automation initiatives couldn't scale

"We were pushing services for our virtualization staff, and site server people, and wondering how we could keep some modicum of control over our DNS, DHCP, and IP address management (DDI) services," explains this healthcare network's network architect.

The entire networking team at this 129,000-person organization is just a small handful of professionals. And they were relying on some Powershell scripts to interface with BlueCat's API.

While the pet project proved the value of automating DDI services, the team began to run into scale problems. "We didn't want code being executed in ten different places. We needed to establish some order."

The solve: Graduating to a zero-touch server build initiative enabled by BlueCat Gateway

"We used BlueCat's Gateway network automation platform to build a number of scalable, fully supported automations. One of those is a cradle-to-grave process that covers everything from server build to decommissioning. It's zero-touch for the distributed network of facilities we serve."

Here's how the automation works: Users make selections in a self-service format through ServiceNow, providing inputs about the new server's location and purpose. Then, Gateway calls VMware's vRealize Orchestrator (vRO) to create the prefix for the host. Next, based on the user's selections, a backend algorithm creates the middle of the host. The suffix is a three- or four-digit number.

Once provided with the hostname, the user can boot up the server, obtain the next available MAC address and IP address from BlueCat, and then go back to ServiceNow and close the request.

"It's a huge win for repeatability and the amount of person-power saved on server builds," the network architect said. "Every one of these more sophisticated automation projects helps us allocate more resources towards improving patient care in other ways."

The lesson learned: Prioritize DDI automation to free up time for more strategic initiatives

More than half (56%) of IT managers report that their teams are overwhelmed with DNS-related tickets and service requests. This has a direct impact on IT's ability to tackle more strategic work. For this healthcare network's IT team, leveraging Gateway along with BlueCat's many integrations was the key to taking their DNS automation initiatives to the next level. It freed up time and resources for more high-value projects.

Along the way, BlueCat's DDI experts worked closely with this organization's 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

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

BLUECAT™

Case Study: Major Financial Institution

February 2019

The Customer

BlueCat engaged one of the world's leading financial institutions about its DNS needs. The company serves over 60 million consumer and small business clients through nearly 10,000 banking and investment centers and one of the largest ATM networks in the world. The company serves clients through operations across the United States, its territories, and more than 35 countries.

The company's network is large and complex, with over 1.85 million active IP addresses in use across headquarters and field offices around the world.

The Challenge

For nearly twenty years, this financial institution operated a split DNS infrastructure. Internal DNS was handled through six disconnected deployments of QIP. Infoblox was used for external DNS.

This balkanized approach had several drawbacks:

Lack of visibility:

The company's administrators were unable to measure the performance or assess usage of DNS resources across the enterprise. As a result, the duplicative effort and higher costs of running parallel systems went unchallenged for years.

Lost or inaccurate data:

The gaps between DNS management systems allowed inaccurate data to creep in over time, resulting in lost data and connections.

Inefficiency:

Without a "single pane of glass" to manage DNS, DHCP, and IPAM resources, the company's administrators spent undue effort translating data and deployments from system to system.

No support for automation:

The lack of an enterprise-wide approach to DNS management made the automation of standard processes such as adding host records or managing IP addresses impossible.

In 2018, Nokia ended active support for its QIP product. Following that announcement, the company attempted to upgrade its QIP instances to the latest active version. This involved a great deal of operational risk due to the size of the bank's database and its multiple audit partitions.

During the upgrade process, it became clear that the stability of the company's network was at risk from continued use of QIP. The network team rolled back to a previous version and began investigating options to unify their DNS infrastructure under a single management platform.

The Solution

As part of its vendor evaluation process, the company set up proofs of concept in its internal lab environment. During this period, the bank's IT administrators and procurement staff learned about the unique benefits of BlueCat:

Data Cleansing:

IT personnel ran tests of a theoretical QIP migration through the DNS management solutions provided by BlueCat, Infoblox, and Efficient IP. Through BlueCat's QIP migration process, BlueCat identified over 30,000 pieces of inaccurate or lost data which both Infoblox and Efficient IP failed to capture.

High Availability:

Given the importance of the company to the global economy, maintaining uptime remains a clear priority. During the evaluation process, BlueCat demonstrated its disaster recovery and high availability functionality in the context of a version upgrade. Given the operational risk associated with QIP upgrades, the ability to quickly and smoothly transition to a new system version with no downtime offered clear benefits.

Automation:

BlueCat also demonstrated its strong support for automation through the DNS Gateway solution. Using its open source workflows for common tasks, BlueCat showed the company's administrators how they could save time and effort while delivering greater functionality to internal stakeholders.

Contract Flexibility:

The company wanted a purchasing model based on what they actually used and consumed rather than a traditional perpetual license approach. Only BlueCat was able to offer a true subscription model with parameters designed with future growth in mind.

The company chose BlueCat because it delivered the right mix of operational functionality and proven expertise in QIP migrations, delivered through flexible contract terms. The network team chose to trust BlueCat with migration of its core infrastructure based on its strong references from other financial services customers and proven record of seamless migrations from QIP.