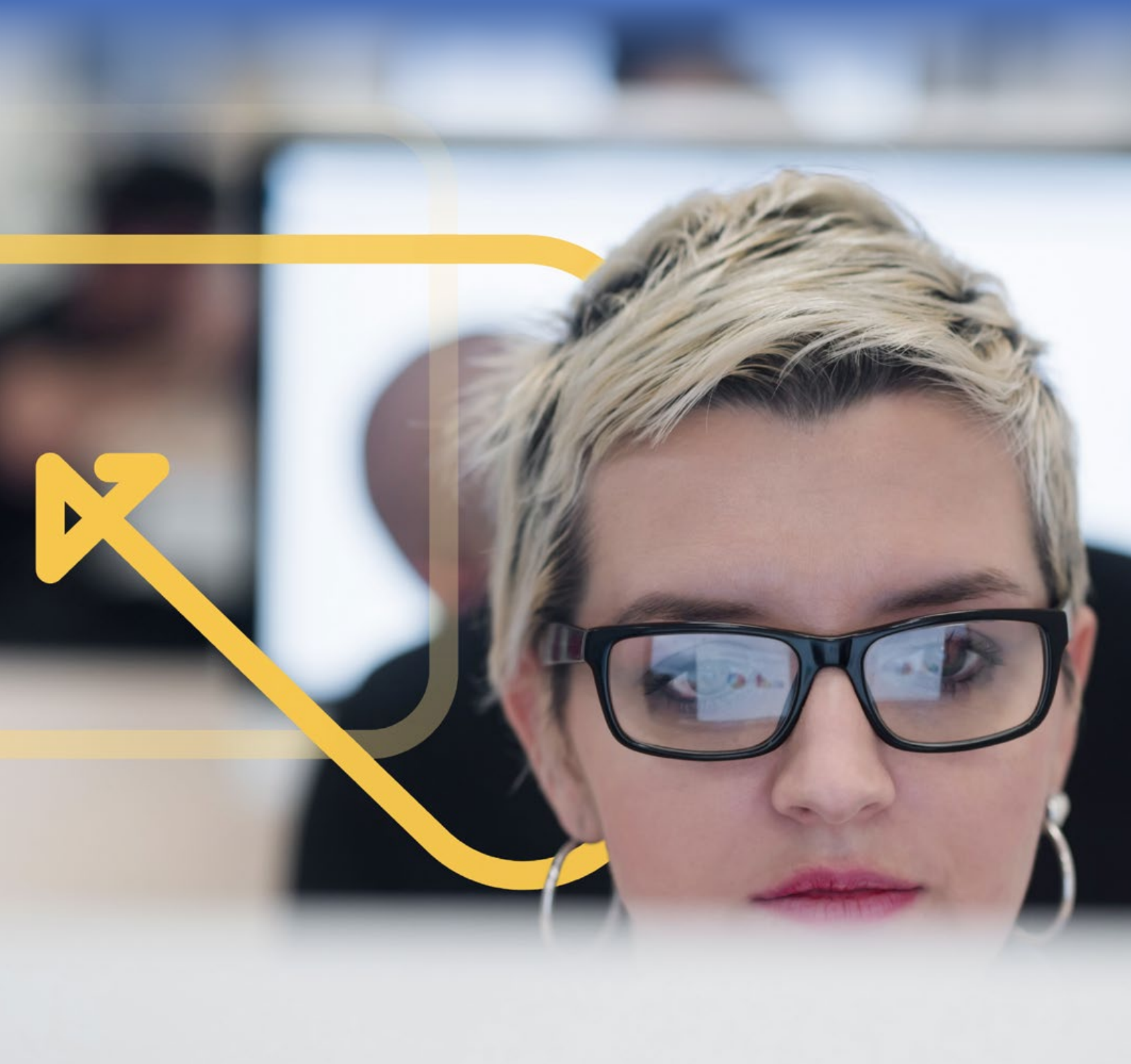
Integrity Case Study – Federal System Integrator



BLUECAT™

The Customer

In April 2018, an acquisition created one of the largest Federally-focused system integrators.

The acquisition posed a daunting challenge to network administrators from both companies. Over the previous few years, the acquired company had been through a series of mergers and spinoffs of its own, leaving its network balkanized and difficult to manage as a single entity. The two pre-acquisition networks were also run in very different ways, creating the additional challenge of bringing two large, complex networks together under a single IT organization.

Beyond the basic issue of rationalizing a combined network architecture, the company was also looking to build its brand around innovation. As the government moves toward a more flexible, value-driven approach to technology, it is already starting to look to Federally focused system integrators to deliver the agile networks which the private sector has long enjoyed. To take advantage of this significant market opportunity, the new company had to build an adaptable, secure, feature-rich network.

Early on, company administrators identified four primary issues to address during the process of network unification and rationalization:

- Manage a complex technology integration
- Provide a consistent end-user experience
- Minimize disruption to network operations while delivering innovative solutions
- Promote and maintain cyber-hygiene

With just ninety days to deliver a combined network, the network team started the process by closely examining core infrastructure requirements.

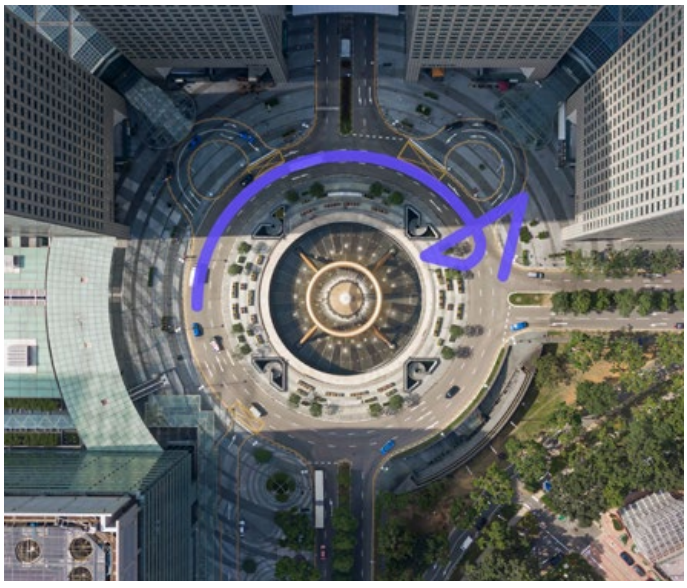
The Challenge

DNS infrastructure quickly emerged as a key priority which required immediate attention. The DNS infrastructure inherited from predecessor companies was a mix of solutions implemented unevenly across different business units.

Many elements of the combined entity already used BlueCat to maximize uptime, minimize errors, and deliver functionality around automation, cloud, and other business initiatives. Other areas of the network still used decentralized, home-grown DNS solutions such as Microsoft and BIND. These delivered basic functionality but were limited in their ability to scale and support higher-level innovation.

The system integrator engaged BlueCat to lay the foundation of its new network infrastructure by centralizing and automating core DNS functions under a single software platform. The team recognized early on that implementing an enterprise-level approach to DNS would enable the system integrator to meet its organizational goals:

- **Manage a complex technology integration:** By providing one platform for management of DNS at the enterprise level, the company would eliminate the need to constantly adjust its home-grown solutions, dramatically simplifying the process of bringing disparate networks under a common architecture and reducing the risk from error-related DNS outages.



- **Provide a consistent end-user experience:** In the legacy environments, users were faced with different network functionality based on their operational unit. By moving to an enterprise approach for DNS, users throughout the network would be able to depend on the high availability and functionality which comes with a centrally managed DNS infrastructure.
- **Minimize disruption to network operations while delivering innovative solutions:** The company engaged BlueCat primarily because of its reputation for superior customer engagement and professional services around complex DNS migrations. BlueCat produced a comprehensive plan for the migration and worked closely with the company to deliver with minimal impact on day-to-day operations. Through the migration process, BlueCat also provided innovative functionality in the form of self-service automation and centralized management of DNS in the cloud.
- During the scoping process, BlueCat and company administrators also began to discuss ways that DNS could assist with the final organizational goal: **promoting and maintaining cyber hygiene.** Since over 90% of malware uses DNS, it made sense that a true enterprise approach to DNS would include the use of this rich data source for security purposes.

The Solution

While both network teams were using BlueCat before the acquisition, they were not on the same version. The two entities had also customized their BlueCat instances over time, resulting in systems geared toward very different desired business outcomes.

To create a common baseline for the migration, BlueCat worked with network administrators to quickly upgrade their existing BlueCat systems. This consultative process began with agreeing on a common set of SLAs and desired business outcomes. The BlueCat team also used the upgrade process to cleanse data from both sides of the network, resulting in a clean data set which would help to scale the system moving forward.

During the deployment process, administrators decided that they wanted Active Directory to be the authoritative source of truth for device-level IP address information. Unfortunately, the Active Directory team was still using spreadsheets to manage DNS records – a process which would naturally slow down BlueCat's automated approach to IP address management.

To bridge this gap, BlueCat engineers came up with a plan to leverage Dynamic DNS (DDNS) to automatically populate BlueCat's IPAM database with records from Active Directory, ensuring that the two systems would automatically sync. This allowed the company to maintain referential integrity of Active Directory as their single source of truth for IP address information while eliminating the need for manual updates to spreadsheets.

The Results

When the company completed its migration to BlueCat, both the network and the Active Directory team found themselves with an abundant new resource: time.

- **Minimal staffing for a larger footprint:** In spite of the highly complex nature of the combined network's DNS infrastructure, the company was able to leverage BlueCat's automation platform to manage the entire estate with just a handful of administrators.
- **Superior service:** Using BlueCat's self-service provisioning of IP addresses, end users on the cloud and DevOps team were able to get the IP addresses they need instantly. By providing instant service, the network team avoided the need for "shadow IT" to fill the gap and maintained full control over DDI resources across the network.
- **Strategic focus:** Since they were no longer managing IP address spreadsheets, provisioning IP addresses for the cloud and DevOps teams, and struggling to simply maintain uptime of their DNS infrastructure, network admins suddenly had time to work on more important things. This ability to focus on more strategic initiatives resulted in the quick promotion of several network admins.

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™