BLUECAT™

Case Study: U.S. Government Laboratory

February 2019

The Customer

BlueCat was approached by one of the U.S. Department of Energy's complex of national laboratories. The laboratory performs work in each of the strategic goal areas of DOE: energy, national security, science and environment.

The laboratory is the nation's leading center for nuclear energy research and development, with 3,900 employees, and a total business volume of $917.1 million.

The Challenge

The Laboratory conducts scientific research on highly sensitive technical areas, and as such its network requires a unique architecture. The vast majority of the Laboratory's workforce is comprised of U.S. citizens, but foreign scientists also work at the lab through cooperative projects and scientific exchange programs.

The Laboratory's network administrators segmented their network to ensure that information was unable to move from the protected enclave of U.S. citizen workers to the enclave used by foreign nationals.

This created an administrative headache, however, as the DNS for both areas had to be managed separately under the Microsoft DNS the lab was using. Spreadsheets were used to keep track of IP addresses and host records, but this was hardly a failsafe method – manual errors frequently caused network outages and increased overall operational risk.

Split administration also lengthened the time it took network administrators to respond to help desk tickets. With a constant flow of foreign researchers and guests, adding and deleting host records took a great deal of time and energy away from more pressing tasks.

The Solution

The Laboratory decided to implement BlueCat's DNS Integrity solution to centralize and automate the management of its core DNS infrastructure.

The BlueCat migration team worked closely with Laboratory administrators to capture, organize, and rationalize the DNS data from each operational enclave. Setting aside blocks of IP addresses for each side of the Laboratory's network, the BlueCat migration team effectively segmented the enterprise while providing the ability to manage DNS resources from a single portal.

The Impact

Using a single point of truth for DNS administration dramatically improved the efficiency and reliability of the Laboratory's DNS infrastructure. Errors and downtime associated with conflicting host records are now a thing of the past – BlueCat's database of DNS data is always up to date, and functions across the U.S. citizen and foreign national enclaves seamlessly.

BlueCat's DNS Integrity solution also improved response times associated with standard DNS management tasks. Adding and deleting host records can now be accomplished quickly and easily, leading to greater productivity for both IT administrators and end users alike. Network personnel are now able to devote more of their time to higher-level strategic tasks.

BLUECAT™