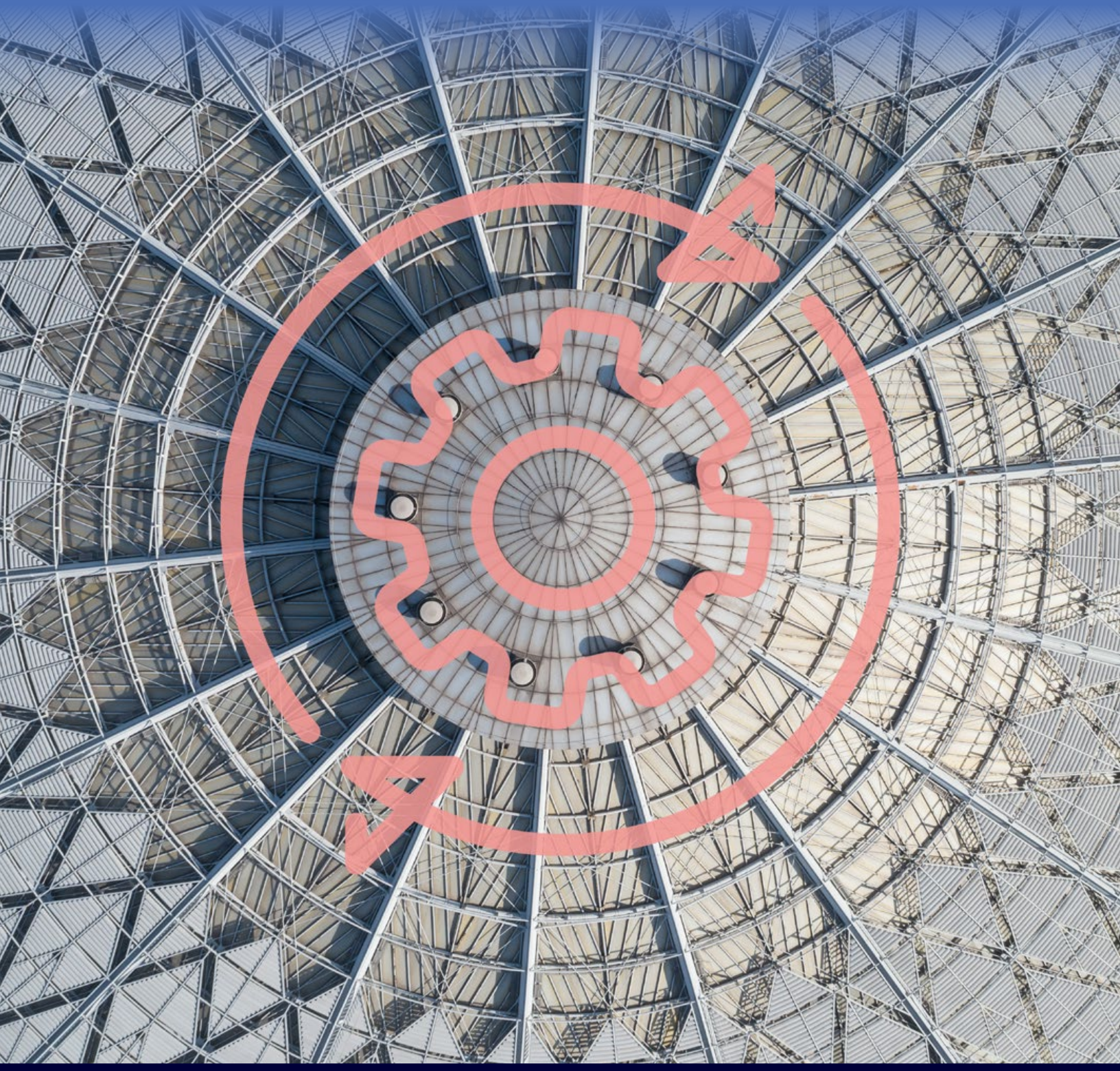
DNS Edge Case Study – Federal System Integrator



BLUECAT™

The Customer

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

The acquisition posed a daunting challenge to the new company's security administrators. 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 secure under a common operational model.

Securing the combined network was particularly important for the newly formed system integrator given its focus on the Federal space. With so many overlapping compliance regimes to account for, the company needed a way to "check the box" with its customers and quickly respond in the event of a security incident to meet stringent SLAs.

Early in the process of combining the two networks, the company identified promotion and maintenance of cyber hygiene as one of its key goals. With just ninety days to deliver a combined network, the network team turned to core infrastructure as a key point of leverage for security. 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 Challenge

The new company was ahead of many of its peers in that it was already leveraging DNS data for security purposes. Over the course of several years, the security team had created a custom system which used elements of open source BIND DNS and Farsight products. This system allowed administrators to aggregate DNS data from multiple sources and use it for analysis of security vulnerabilities.

While the system was truly innovative and valuable to the security team, it came at a tremendous cost in terms of administrator time and effort. A single security staffer was stuck updating domain lists on a daily basis and maintaining the complex, interlocking BIND rules necessary to keep the system up and running.

The system was able to provide a great deal of visibility into DNS logs, but the process of associating DNS activity with a source IP was still manual. In the event of an incident, security administrators were known to roam from office to office, consulting the sticky notes attached to each computer to see if they matched with the DNS log data they had on file. Using this process, it often took weeks to find "patient zero" of any particular incident.

During the acquisition period, the administrator of this system decided to take another job. Not only did this essentially freeze the functionality of the custom-built security system, but it also led to several internal compliance problems as security administrators were suddenly unable to provide the definitive DNS data end-users required.

The Solution

The security and network teams researched many options for DNS security during the transition period. Many of the options they found were deployed at the network boundary, providing insight into external queries but preventing any visibility into internal, "east-west" traffic. To provide device-level insights, many of these solutions required on-device agents. The teams eventually selected DNS Edge because it provided full visibility into network traffic without the need for agents.

The company deployed a proof of concept for DNS security using its DNS Edge product in 2019. DNS Edge was deployed over 10,000 IP addresses in this initial phase, and is now expanding to 35,000 in full deployment mode. DNS Edge was also placed in the company's center of excellence for approved technologies.

BlueCat worked closely with the security and network teams to integrate DNS Edge into their broader cybersecurity framework. BlueCat adapted its SIEM integration to feed directly into ArcSight, the company's chosen tool for monitoring cybersecurity threat data.

BlueCat also took a series of existing threat feeds used by the company (from both internal and external sources) and integrated them into the policy engine for DNS Edge. This allowed the teams to not only use existing data sources they were already used to, but also provided the new visibility into network activity. Since DNS Edge works at the "first hop" of any network query, the security team was able to block malicious activity at the client level for the first time.

In addition to the company's existing threat feeds, BlueCat worked with administrators to establish a series of custom security policies which would monitor, flag, or block anomalous activity at the client level. These policies were based on patterns of anomalous activity on the company's own network as observed by DNS Edge during the proof of concept phase, and tailored to block specific types of traffic based on device, network location, DNS query type, or any number of other risk factors.

Results

The company's security administrators quickly discovered the value of granular DNS data to their daily operations. With full visibility into both internal and external traffic , the security team cut the time needed to locate the source of security incident dramatically – from several weeks to just a few minutes.

All the time they once used to consult sticky notes and IP address spreadsheets is now used to process a greater volume of security threats. The granular information provided by DNS Edge also allows the security team to craft finely tuned security policies which can be deployed consistently across the entire enterprise.

The company found so much strategic and tactical value in DNS Edge that the internal champion was promoted for leadership in identifying the solution and driving it forward.

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™