BLUECAT™

Case Study: Medical Technology Company

February 2019

The Customer

BlueCat was approached by a leading medical technology company with nearly $20 billion in annual revenue and over 70,000 employees around the world. The company's primary business is supplying hospitals and clinics with a wide variety of medical devices.

All of the company's medical devices require periodic maintenance. In the past, it employed a large team of Field Service Engineers which visited medical facilities on a set schedule to service and troubleshoot devices. In recent years, the company decided to connect all of its devices to the internet, enabling remote diagnostics and updates. This allows a smaller number of Field Service Engineers to effectively maintain a larger fleet of devices.

The Challenge

Managing network connections between medical devices deployed in the field and the company's service staff proved to be a multifaceted challenge:

Compliance: Under the Health Insurance Portability and Accountability Act (HIPAA), all of the connections between medical devices and the company's servers had to be encrypted. This involved creating and managing separate VPN tunnels for over 15,000 field-deployed devices.

Network Conflicts: The company's devices rely on the IT infrastructures of the medical centers and clinics where they are deployed. The devices are assigned IP addresses by the network teams of each facility, usually without any coordination. This introduces the potential that devices in different facilities will be assigned the same IP address, making remote monitoring and maintenance much harder to track.

Visibility: The company's network infrastructure has been shaped over time by multiple mergers, acquisitions, strategic initiatives, and partnerships. On-prem assets are a tangle of directly administered data centers and services managed by third party providers. Maintaining visibility into the DNS of this complex enterprise is a significant challenge. The company recently started to use the AWS cloud for much of its internal compute. As its use of the cloud grows in volume and sophistication, the company will want to manage its cloud DNS from a central location.

The company's Microsoft-based DNS did not deliver the range of functionality required by such a complex, compliance-based network architecture. In order to deliver the efficiency of automated processes, the company needed a single point of truth for its DNS infrastructure – one which supported the use of APIs and automation.

The Solution

To address its many DNS-related challenges, the company turned to BlueCat. Working with BlueCat's migration team, the company transitioned its scattered on-prem DNS resources from Microsoft to DNS Integrity. A significant part of the migration effort involved bringing legacy systems and namespaces under a single DNS administration portal, organizing and accounting for dispersed data sets across the enterprise. This laid the foundation for the company to tackle the larger challenge of managing its connections to devices in the field.

Using DNS Integrity's robust API, the company's application development team then built a custom portal to manage remote devices through the BlueCat back-end. This portal uses Network Address Translation (NAT) and a Dynamic Multipoint Virtual Private Network (DMVPN), automatically integrating host records from remote devices with the BlueCat Address Manager.

The Outcome

With the company's custom-built portal running through BlueCat's API, the company is now able to automatically establish and maintain remote connections with medical devices without the need to constantly adjust IP addresses in coordination with hospital IT teams.

BlueCat's centralized system allows network administrators to automate IP provisioning for individual devices, set aside blocks of IP addresses for entire medical facilities, and maintain an accurate DNS database that is updated in real time.

Automating the DNS back-end also gives administrators the ability to manage the 15,000+ VPN connections required by HIPAA from a single portal – something that was impossible under the previous Microsoft-based architecture. The system also offers a more reliable architecture which avoids the errors and downtime naturally associated with manual DNS management.

Where the company's Field Service Engineers used to visit customer sites on a regular rotation to service and maintain medical devices, they can now perform the same tasks through the company's custom-built portal which runs on the BlueCat API. Field Service Engineers now have the ability to perform complete audits of device functionality by scanning ports, performing remote launches, and updating firmware – all without the need to go on site.

Doing so requires a much smaller team which operates on more efficient timeframes. The cost and resources associated with on-site visits are now the exception rather than the rule, offering significant operational savings for the company.

"BlueCat's platform is highly stable" says the company's lead DNS administrator. "With BlueCat's API, we were able to create a custom platform which helps us manage resources at scale, saving time and money."

BLUECAT™