CASE STUDY

Geisinger Health System

The Customer:
Geisinger Health System operates more than 15 hospitals, medical research centers and clinics in Pennsylvania.

The Challenge:
The need to bring visibility, control and security to a distributed network that supports health services for more than two million people

The Solution:
- Infoblox Grid™ technology
- Infoblox DDI and DHCP Fingerprinting
- Infoblox Reporting
- Infoblox DNS Firewall

The Results:
- Simple, centralized management
- Scalability and rapid onboarding of new locations
- Visibility to accurately control every aspect of the devices connecting to the network
- Vastly improved DNS security to protect medical devices

Geisinger

The Customer

Geisinger is an integrated health-services organization widely recognized for its innovative use of the electronic health record and for the development and implementation of innovative care models. The system serves more than 2.6 million residents throughout 44 counties in central and northeastern Pennsylvania.

The Challenge

Geisinger became an Infoblox customer in 2011. Before that, the healthcare provider used Alcatel-Lucent VitalQIP to manage its Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services. But like many VitalQIP users, Geisinger was looking for an alternative. In addition to a costly per-IP-address licensing scheme, VitalQIP wasn't keeping up with emerging requirements. (It was in 2011 that Gartner reported that VitalQIP customers were voicing concerns about how attentive Alcatel-Lucent was to their needs[1], and just recently, the company sold 80 percent of its Enterprise Division—which includes the VitalQIP product.)

According to Rich Quinlan, one of three technical analysts responsible for DNS and DHCP services for Geisinger and its affiliates, "The decision of what to replace VitalQIP with came down to Microsoft or Infoblox. We felt that Infoblox was best of breed, and that it offered us the most flexibility and centralized administration for our future plans."

He goes on to explain that Geisinger's network can have as many as 20,000 users, and at any given time can have the same number of devices utilizing DNS and DHCP services. "We have a huge variety of systems," he says, "from Food and Drug Administration-controlled devices that we have to keep separated, to the personal devices of the staff and patients."

The Solution

Now Geisinger has a solution based on patented Infoblox Grid™ technology. It includes Infoblox DDI, Reporting, DNS Firewall, and DHCP Fingerprinting. The Grid Master for the system is a high-availability (HA) pair of Infoblox 2220 appliances. DNS and DHCP functions are handled by Infoblox 800 and 1400 series appliances, also in HA pairs.

1. "MarketScope for DNS, DHCP and IP Address Management," Gartner RAS Core Research Note G00210742, Lawrence Orans, 24 March 2011.

"The decision of what to replace QIP with came down to Microsoft or Infoblox. We felt that Infoblox was best of breed, and that it offered the most flexibility and centralized administration for our future plans."

Rich Quinlan,
Sr. Technical Analyst, Geisinger Health System

The Result

When asked what the solution delivers, Quinlan cites a range of benefits. "Bringing a new hospital onboard is quite easy now," he says. "We define the address space that we are going to use, point their devices toward ours, and we are off and running in very little time. Infoblox gives us good role-based access to delegate tasks to various groups. It also gives us

a very quick and easy-to-use platform for managing everything from a single pane of glass. Scalability for the future is definitely there. And the DNS, DHCP, and IP address management functionality is really unmatched by any other product."

He also mentions visibility and high availability. But one component he seems particularly impressed with is Infoblox DNS Firewall, a unique solution that protects against malware-driven DNS queries to malicious domains by disrupting the ability of infected clients to communicate with botnets or command-and-control servers.

"We are doing an evaluation of DNS Firewall, and during that evaluation—even though we have incident detection and prevention systems and firewall logging—we detected a federally controlled device that was attempting to communicate with a known command-and-control server," he says. He goes on to explain that DNS Firewall detected the outbound communication, and Infoblox DHCP Fingerprinting—which captures the device type for the IP address issued as part of the DHCP process—enabled Quinlan's team to quickly and accurately identify the offending device so that the threat could be contained before it spread to other devices.

Quinlan underscores the seriousness of this kind of threat. "In spite of all the conventional steps we take to protect our internal network, patient care could still be affected. We could have an entire hospital full of useless ultrasound devices because one was brought in with a virus and we have no control over them. And if it was able to exfiltrate data, we would have a Health Insurance and Portability Accountability Act (HIPAA) compliance issue."

So DNS Firewall plugs the hole that conventional security measures leave in Geisinger's defenses. It also protects against media access control (MAC) spoofing, which Quinlan points out is important because if an attacker tries to make a rogue device look like one of Geisinger's trusted devices, Infoblox gives IT the ability to accurately and quickly identify and quarantine such devices before they can affect patient care.

Quinlan concludes by saying, "Our partnership with Infoblox has been excellent. The support, both sales and technical, has been on the ball. And our solution keeps getting better." He points out that at first he was just able to better manage IP addresses. But now the solution has evolved so that, for instance, if somebody asks how many Apple devices are using the guest network, he can find out using DHCP Fingerprinting and report the statistic using Infoblox Reporting.

"So it continues to be a good investment," he says, "and it has been one of the most reliable systems that we have in the entire organization. We have had zero unexpected downtime in the three years that it's been in place, and that's very rare in this day and age. I can sleep better at night knowing that we are not going to have a system failure."

For more information, please contact your Infoblox representative or visit www.infoblox.com.

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com